

United States District Court

EASTERN District of CALIFORNIA

FILED
Jan 13, 2025
CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

In the Matter of the Seizure of
(Briefly describe the property to be seized)

1,285,540.357235 USDT held in the Ethereum account
0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7.

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

CASE NUMBER: 2:25-sw-0032 CKD

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the BRITISH VIRGIN ISLANDS is subject to forfeiture to the United States of America (*describe the property*):

1,285,540.357235 USDT held in the Ethereum account
0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7.

The property is subject to seizure pursuant to 18 U.S.C. § 981(b) and 982(b), and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), and 982(a)(1), and 28 U.S.C. § 2461(c), concerning violations of 18 U.S.C. §§ 1343 and 1956.

The application is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

/s/

Applicant's signature

David Berry, Special Deputy U.S. Marshal,
USSS Cyber Fraud Task Force,
Criminal Investigator, Santa Clara County
Office of the District Attorney

Printed name and title

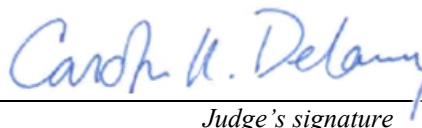
Sworn to before me and signed telephonically.

January 13, 2025 at 5:52 pm

Date

Sacramento, California

City and State



Judge's signature

Carolyn K. Delaney, U.S. Magistrate Judge

Printed name and title

United States District Court

EASTERN District of CALIFORNIA

In the Matter of the Seizure of
(Briefly describe the property to be seized)

1,285,540.357235 USDT held in the Ethereum account
0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7.

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

CASE NUMBER:

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the BRITISH VIRGIN ISLANDS is subject to forfeiture to the United States of America (*describe the property*):

1,285,540.357235 USDT held in the Ethereum account
0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7.

The property is subject to seizure pursuant to 18 U.S.C. § 981(b) and 982(b), and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), and 982(a)(1), and 28 U.S.C. § 2461(c), concerning violations of 18 U.S.C. §§ 1343 and 1956.

The application is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.



Applicant's signature

David Berry, Special Deputy U.S. Marshal,
USSS Cyber Fraud Task Force,
Criminal Investigator, Santa Clara County
Office of the District Attorney

Printed name and title

Sworn to before me and signed telephonically.

January 13, 2025 at 5:52 PM

Date

Sacramento, California
City and State

/s/

Judge's signature

Carolyn K. Delaney, U.S. Magistrate Judge
Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEIZURE WARRANTS**

I, David Berry, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND PURPOSE OF AFFIDAVIT

1. I submit this affidavit in support of an application for the issuance of three seizure warrants for cryptocurrency assets held in two Tether accounts on the Tron network and one Tether account on the Ethereum network, collectively referred to hereinafter as the “Target Property,” to wit:

- a. 500,001.2 USDT held in the Tron account
TNihvNZfFYdSjLWyEHIPXQ2u28oXHN1PNu, hereinafter referred to as
“Subject Account 1,” and;
- b. 1,000,100.145687 USDT held in the Tron account
TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF, herein referred to as “Subject
Account 2,” and
- c. 1,285,540.357235 USDT held in the Ethereum
account0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7, herein
referred to as “Subject Account 3.”

2. The property to be seized and the seizure procedure is described in the following paragraphs and in Attachment A.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that unknown subjects have violated Title 18, United States Code, § 1343 (Wire Fraud) and laundered the proceeds of that activity in violation of Title 18, United States Code, § 1956(a)(1)(B)(i) (Money Laundering). There is also probable cause to believe that the Target Property contains the proceeds of the wire fraud scheme described below. Accordingly, the fraud and money laundering proceeds, totaling approximately 1,415,680 USDT are subject to seizure and forfeiture pursuant to Title 18, United States Code, § 981(a)(1)(C), and Title 28, United States Code, § 2461(c). Moreover, as indicated herein, there is probable cause to

believe that the Target Property has been used to launder the funds of criminal activity.

Accordingly, there is also probable cause to seize the Target Property as funds involved in money laundering transactions, pursuant to Title 18, United States Code, §§ 981(a)(1)(A) and 982(a)(1).

4. The facts in this affidavit come from my personal observations and knowledge, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. All dates are on or about the date specified. All amounts are approximate.

5. I accordingly request that the Court authorize the attached warrants for seizure of the assets described herein.

AGENT BACKGROUND

6. I am an “investigative or law enforcement officer” of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am a Special Deputy United States Marshal, sponsored by the United States Secret Service, and empowered by law to conduct criminal investigations and make arrests for offenses enumerated in Title 18 of the United States Code.

7. I am currently employed as a Criminal Investigator with the Santa Clara County Office of the District Attorney and have been so employed since December 2012. Since August 2015 I have been assigned to the Regional Enforcement Allied Computer Team (“REACT”) Task Force, where my primary duties include the investigation of technology-related crimes with an emphasis on cyber-facilitated fraud and theft. I attended the Peace Officer Standards and Training (“POST”) Basic Police Academy in San Jose, California in 2003, where I received formal training in the investigation of a variety of crimes. I have been a sworn peace officer

since 2003, during which time I have participated in hundreds of criminal investigations involving various types of computer crimes. I have earned a certificate in the Investigation of Computer Crimes from the Robert Presley Institute of Criminal Investigations. From March through September 2017, I participated in a full-time fellowship with the FBI's National Cyber Investigative Joint Task Force, where I worked with various United States Government organizations to obtain additional training and experience in conducting technology-related investigations, including those involving cryptocurrency. I have also attended numerous other courses during which I received training in the investigation of technology-related crimes and the collection of digital evidence for use in criminal investigations. I have taken several formal training courses regarding cryptocurrency and its application to criminal investigations, have conducted dozens of investigations involving the criminal use of cryptocurrency, and have taught classes on this topic to other law enforcement investigators throughout the United States on numerous occasions. I have investigated dozens of cases of cryptocurrency theft, including many involving fraud schemes like the one described herein. I have been recognized as an expert in Santa Clara County Superior Court on the subjects of cryptocurrency investigation and the fraud scheme described herein.

8. Title 18, United States Code, Sections 981(b)(2) and (3) provide that seizure warrants shall be made pursuant to a warrant issued in the same manner as provided for a criminal search warrant under the Federal Rules of Criminal Procedure. Moreover, seizure warrants may be issued in any district in which a forfeiture action may be filed and may be executed in any district in which the property is found. Federal Rule of Criminal Procedure 41 governs the issuance of criminal search and seizure warrants.

9. Title 28, United States Code, Section 2461(c) provides that the procedures (including seizure warrants) in Title 21, United States Code, Section 853 control criminal forfeiture. Section 853(f) of the same title provides that the government may request a warrant for the seizure of property for forfeiture in the same manner as it may seek a search warrant. Title 18, United States Code, Section 982(b)(1) also provides that seizures for criminal forfeiture shall be made pursuant to a warrant issued in the same manner as provided for a criminal search warrant under the Federal Rules of Criminal Procedure, and cross-references Title 21, United States Code, Section 853. This warrant seeks seizure authority under both the criminal and civil forfeiture statutes.

10. Title 21, United States Code Section 853(f) provides that a court may issue a criminal seizure warrant when it “determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a[] [protective] order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture.” As set forth further below, there is a substantial risk that the Target Property will be withdrawn, moved, dissipated, or otherwise become unavailable for forfeiture unless immediate steps are taken to secure them. I therefore submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that the Target Property will remain available for forfeiture.

11. One of the chief goals of forfeiture is to remove the profit from crime by separating the criminal from his or her dishonest gains, and to divest criminal actors from the apparatus allowing them to engage in criminal activity. *See United States v. Newman*, 659 F.3d 1235, 1242 (9th Cir. 2011); *United States v. Casey*, 444 F.3d 1071, 1073 (9th Cir. 2006). To that end, in cases involving a money laundering offense, the forfeiture statutes connected to money

laundering offenses permit the government to forfeit property “involved in” money laundering. Such property includes “untainted property” commingled with “tainted” property, when that untainted property is used to facilitate the laundering offense, such as by obscuring the nature, source, location, or control of any criminally derived property. *See* Title 18, United States Code, Sections 981(a)(1)(A), 982(a)(1); *see also United States v. Kivanc*, 714 F.3d 782, 794-95 (4th Cir. 2013); *United States v. Huber*, 404 F.3d 1047, 1056-1058 (8th Cir. 2005).

12. Based on my training, experience, and the information contained in this affidavit, there is probable cause to believe that funds in the Target Property are subject to both civil and criminal forfeiture as proceeds traceable to a wire fraud scheme, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c). The balance of the Target Property is subject to both civil and criminal forfeiture as property involved in money laundering, pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1). The balances of the virtual currencies in the Target Property are therefore subject to civil and criminal seizure.

CRYPTOCURRENCY AND VIRTUAL CURRENCY EXCHANGES

13. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar but are generated and controlled through computer software. Bitcoin is currently the most well-known virtual currency in use.

14. Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters.

15. Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the

address. An address is somewhat analogous to a bank account number and is represented as a string of letters and numbers up to 40 characters long. Users can operate multiple addresses at any given time, with the possibility of using a unique address for every transaction. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address. Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

16. A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

17. Many virtual currencies publicly record all of their transactions on what is known as a "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

18. **Stablecoins**: Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDC and USDT are stablecoins pegged to the U.S. dollar.

Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

19. **Tether (USDT):** Tether Limited (“Tether”) is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USD Tether (“USDT”) tokens. USDT is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a “stablecoin.” USDT is hosted on the Tron and Ethereum blockchains, among others.

20. **Tron (TRX):** Tron (“TRX”) is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses smart contract technology. The public ledger is the digital trail of the Tron blockchain, which allows anyone to track the movement of TRX and tokens such as USDT.

21. **Ether (ETH) and Ethereum:** Ether (“ETH”) is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a network called Ethereum that uses smart contract technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH and tokens such as USDT.

22. **USD Coin (USDC):** USD Coin (“USDC”) is a blockchain-based a stablecoin. USDC is hosted on the Ethereum network, among others. USDC is issued by Centre, a company headquartered in the U.S. USDC is connected to Coinbase and Circle, cryptocurrency exchanges registered in the U.S.

23. **Smart contracts:** Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract’s code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using blockchain protocols such as Ethereum and Tron to maintain

transparency. Multiple cryptocurrencies, including USDT, can utilize the Ethereum or Tron blockchains to take advantage of this technology. Smart contract technology is one of the distinguishing characteristics of Ethereum and Tron and is an important tool for companies or individuals executing trades on these blockchains. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum or Tron blockchain and is both trackable and irreversible.

24. **Decentralized finance application:** One of the many applications of smart contracts on blockchains such as Ethereum is to facilitate financial transactions involving cryptocurrency that do not rely on a centralized custodial service to execute. Such applications are decentralized in nature as they rely on pre-established smart contracts (rather than trusted intermediaries) to execute code automatically in response to certain inputs. These applications are commonly used to “swap,” for example, Ethereum for USDT, or USDT for another Ethereum token, such that one asset is sent from the address and an equivalent value (less fees) of the corresponding asset is received into the same address nearly instantaneously, within the same transaction. Services utilizing these mechanisms are often referred to as “decentralized finance applications.”

PROBABLE CAUSE

25. This investigation was initiated from a fraud report received by the REACT Task Force, a participating member of the USSS San Francisco Field Office’s Cyber Fraud Task Force, from “RB”, a 62-year-old resident of Grass Valley, California, in the Eastern District of California. In or about June through August of 2024, RB fell victim to an ascending investment

fraud scheme known as “Pig Butchering”, which resulted in a total loss of approximately \$167,000 to RB.

26. The investment scam detailed in this affidavit is consistent with Pig Butchering scams in general. Pig Butchering originated in China in 2019 and often begins with a perpetrator sending a victim an unsolicited text message, typically via WhatsApp or a social media/dating website. From the initial message, the perpetrator develops an intimate relationship with the victim using manipulative tactics similar to those used in online romance scams. Pig Butchering schemes frequently originate in various locations throughout Southeast Asia, including, but not limited to, Hong Kong, Myanmar, Cambodia, Malaysia, Thailand, and Singapore.

27. Pig Butchering victims are referred to as “pigs” by the perpetrators, because the perpetrators will use elaborate (and often romantic) storylines to “fatten up” victims into believing they are in a trusting relationship. Once the victim reaches a certain point of trust, they are brought into a cryptocurrency investment scheme and provided fabricated evidence to bolster the scheme’s legitimacy and eliminate any skepticism the victim may have about the investment (i.e., the ongoing scam). Victims are provided fake investment platforms via a website or mobile application that showcases fictitious investment gains. In reality, the website or application has limited functionality and does not provide the user any access to a cryptocurrency wallet. The perpetrators may also provide fake transaction photos to create the false impression the perpetrators are contributing their own funds to the victim’s initial investment. However, the investment gains displayed on the investment platform website or mobile application are fabricated. In truth, the investment platform does not exist.

28. The perpetrator encourages victims to invest more funds into the platform, with the promise of higher returns. Victims are often allowed to make small initial withdrawals to

bolster the perception of control over the assets, as part of the effort to increase trust in the platform and encourage larger investments. When significant withdrawals are attempted, however, they are not allowed. Various excuses are given for blocked withdrawals, often involving fees and taxes that are due (and require "fresh money" rather than being paid from supposed gains) and sometimes alleging that suspected misconduct has caused a freeze of the account for compliance purposes. Victims are ultimately unable to withdraw their funds regardless of how much more money is contributed to the platform, and their investment funds are stolen from them. The financial loss causes the victims financial, personal, and emotional ruin and is referred to by the perpetrators as “butchering” or “slaughtering” the victims.

29. The efforts to defraud RB were evident within approximately two weeks of the perpetrator’s initial message on Facebook, as RB purchased USDT, USDC and Bitcoin from cryptocurrency exchanges Crypto.com and Strike and transferred it into the fraudulent trading application, “BIT.”

30. The “BIT” application used to defraud RP appears to be a play on the legitimate cryptocurrency trading business with the same acronym, “BIT”. The acronym “BIT” used hereafter refers to the fraudulent platform, not the legitimate company that was not involved in this caper.

31. The fake BIT platform gave the illusion that RP had huge gains from high-frequency trading. However, the perpetrator offered various excuses—and even demanded more money—when RB tried to withdraw funds. RB contributed a net total of approximately \$165,000 worth of cryptocurrency to the investment scheme before realizing it was a scam.

A. “BIT” Impersonation Wire Fraud Scheme

32. The summary of RB's investment in the BIT platform is based on RB's statements, screen shots provided by RB of his interactions with the perpetrators and the bogus investment platform, records obtained from the cryptocurrency exchange Strike pertaining to RB's account, and information viewable on public blockchains.

33. In or about June of 2024, RB was participating in a motorcycle enthusiast Facebook group when he was messaged by a female identified as "Linda GAO." GAO claimed to own a motorcycle and they chatted a few times on Facebook, including video chats. After a matter of days, GAO asked that they move the chat to WhatsApp.

34. RB later noticed that some of the wording was strange, so he asked if GAO was using a translator, and GAO confirmed she was. In retrospect, RB thinks he likely chatted with different people at different times based on the changing personalities he encountered chatting with GAO.

35. Based on my knowledge and experience conducting cryptocurrency fraud investigations, I know that these criminal organizations often operate in multiple tiers of responsibility. Most often, the individual that communicates directly with the victim is on a lower tier of responsibility in the criminal organization, whereas individuals receiving funds at the end of the scheme are those who profit the most and are typically higher in the criminal organization's hierarchy.

36. Based on my knowledge and experience in investigating cyber fraud schemes, GAO is most likely not the person portrayed to the victim during their WhatsApp conversations and may actually be a role played by multiple individuals. After a week or so, the conversation with GAO shifted to money. GAO claimed to have a degree in economics and started talking about cryptocurrency. GAO told RB she had made a lot of money trading cryptocurrency options

and offered to help RB make money doing the same. RB confided in GAO that his father had dementia and he needed money to pay for his father's care.

37. At GAO's direction, RB downloaded the TrustWallet cryptocurrency wallet application to his mobile device and used it to connect to a platform called "BIT" accessed via a URL provided by GAO. He created an account on the BIT platform which he always accessed via TrustWallet. Based on my training and experience, I know that perpetrators of Pig Butchering scams provide links to applications and website that function and appear like legitimate cryptocurrency platforms. The apps and sites display information that include account numbers, cryptocurrency wallet addresses, investment amounts and gains, and deposit/withdrawal functions. The application featured graphics and layouts consistent with most extant smartphone currency trading applications. The perpetrators routinely adjust the displays as they see fit through the course of the scam.

38. The site's URL often changed, approximately monthly. The site's initial URL was <https://cntzcy.com>. On July 30, 2024, RB received an email from the platform's customer service email stating that due to a "hacked malicious attack," the web platform's domain changed to <https://cdsslt.com>. On August 28, 2024, RB received an email from the platform customer service email stating that the platform's web domain had changed to <https://oluarr.com>, again due to another "hacked malicious attack."

39. Based on my training and experience, I know it is common for perpetrators to change the domain names of the web sites where their bogus site is hosted in order to maintain continuity of operations when victim reporting leads to the initial domain being identified online as fraudulent, or blocked or taken down by webhost providers, registrars, or government authorities. In addition, it would be unusual and counterproductive behavior for a legitimate

business to frequently change its web address, or to use such different URLs that appear to have no relationship to the actual name of the company or service.

40. GAO showed him how to use BIT and explained that there were different tiers of investment, where the expected rate of return from investing in different pools of options (for example the 30-second pool, 60-second pool, or 90-second pool) increased with the amount of money invested. By investing more, higher rates of return could be achieved.

41. RB sent some cryptocurrency from his preexisting account at the exchange Crypto.com to BIT, using the deposit address provided to him by BIT. The cryptocurrency was purchased using credit cards linked to his Crypto.com account and wire transfers from his Bank of America account. Between July 14 and July 21, 2024, RB sent at least 38,150 USDC from his Crypto.com account to his own unhosted wallet, and from there to the address provided by BIT to deposit the assets into his BIT account.

42. RB experienced disruptions with the Crypto.com transactions and told GAO, who urged RB to instead use the Strike exchange to avoid the barriers created by Crypto.com. GAO guided RB through the transition to Strike, and RB registered an account at Strike for the purpose of investing in BIT.

43. On or about July 25, 2024, RB sent \$5,000 from his Bank of America account to his Strike account. RB purchased \$5k worth of BTC and sent it to the address provided by BIT to make a deposit into his account. At one point, after sending funds from Crypto.com and Strike, RB had a \$60k balance of his own funds in the BIT account. On or about August 13, 2024, RB successfully withdrew those funds from his BIT account to his Strike account and then withdrew \$59,716.60 from his Strike account to his Bank of America account. This experience convinced

RB that GAO's investment opportunity was sincere and legitimate, because RB believed if they were going to steal his \$60k, they would have kept it.

44. GAO offered to loan RB \$50k to propel him into a higher tier of return on BIT, and when RB agreed to the arrangement, RB's funded balance on BIT showed a \$50k increase of cryptocurrency. GAO later purportedly added another \$150k worth of loans to RB's account, as reflected in his BIT balance. The cryptocurrency GAO transferred to RB appeared as if it had been transferred from Crypto.com. GAO told RB that a big trade opportunity was forthcoming but would only be open for a short period because of increased risk factors connected to election politics. GAO ultimately convinced RB that he needed another \$160k to step up into the next tier. Between GAO's supposed loans to RB, the funds RB personally invested, and the purported investment gains, RB's account reflected a sufficient balance to reach the next tier.

45. On or about August 16, 2024, RB wired \$160,000 from his Bank of America account to his Strike account. RB used the \$160,000 in his Strike account to purchase 2.69292824 BTC, which RB sent to his BIT account (to an address provided by BIT). By August 27, 2024, his account on BIT appeared as if he had over \$924,000 worth of USDT. GAO told him that trades would be paused for a while because of political turmoil surrounding the election, and suggested he cash out.

46. In mid to late August, RB requested a withdrawal of approximately 674,000 USDT from BIT, but BIT showed that the withdrawal was "pending clearance" or "on hold." The next morning, on or about August 21, 2024, BIT's message changed to "Contact customer service" and indicated RB's account was locked because RB had input the wrong receiving address. However, RB compared screen shots he entered and confirmed he had input the correct address. BIT's message now showed a missing digit.

47. RB contacted BIT's online service assistant who advised RB to deposit 20% of his balance (approximately \$180,000) to unfreeze the funds. If RB did not comply and deposit more funds within three days, the balance of his account would be donated to the United Way. At this point, RB concluded that the investment was a scam and contacted law enforcement.

B. Cryptocurrency Addresses and More Victims of the BIT Scam

48. During the investment scam, BIT provided instructions to RB to transfer funds to a series of cryptocurrency addresses, which are reproduced below:

- a. The Bitcoin addresses 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV, 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT, and bc1qjh6dc0scfu9vdyf2yjdjhj96uvlvtf6tdhhw8ml were provided for BTC deposits. His largest and final deposit of 2.6921677 BTC was sent to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV and was reflected in his BIT account balance. This address was also the source of the BTC withdrawals he successfully received from BIT.
- b. The Ethereum address 0xE073907d67A125DB8Fac7ea4719B3AaB94752D03 was provided for USDC deposits. RB made two USDC deposits to this address that were reflected in his BIT account balances.
- c. The Ethereum address 0xC46ABF247b6a0d86FF178561D0893ddD0f00C23e was provided for both USDT and USDC deposits. RB did not make actual deposits to this address.
- d. The Ethereum address 0xE6626588bAea62C2229783D082d362c9525a1296 was provided for USDT deposits. RB did not make actual deposits to this address.
- e. The Tron address TJTWrPyts7ahu22iWupAfeGKDojqy9nLFF was provided for USDT deposits on the Tron network. RB did not make actual deposits to this address.

49. I connected the above addresses to other related victim complaints on the Federal Bureau of Investigation's ("FBI's") Internet Crime Complaint Center, known as IC3 (<http://www.ic3.gov>). The following seven IC3 reports, also victims of purported Pig Butchering scams, reference one or more of the same unique identifiers connected to RB's scam:

- a. WS, a resident of Lillington, North Carolina, reported losing \$23,468 worth of cryptocurrency in July and August, 2024 after sending Bitcoin to the address 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV used by a platform identifying itself as BIT and using the URL <https://cdsslt.com>. The description of the scam was consistent with pig butchering.
- b. PT, a resident of Forsyth, Georgia, reported losing \$85,200 in May and June of 2024 after sending USDT to 0x211d18f4262383911500e1298e02c4865e91abe2 used by a platform using the web domain Bit-world.cc. The USDT was forwarded from that address to 0xE073907d67A125DB8Fac7ea4719B3AaB94752D03. The description of the scam was consistent with pig butchering.
- c. TM, a resident of Roebuck, South Carolina, reported in July 2024 having lost at least \$2,000 in cryptocurrency using a site identifying itself as BIT and using the web domain OULARR.com. The description of the scam was consistent with pig butchering.
- d. MW, a resident of Concord, North Carolina, reported in September 2024 having lost \$50,000 to a scam identifying itself as BIT after meeting a woman on a motorcycle enthusiast Facebook group in July. The description of the scam was consistent with pig butchering.
- e. RJ, a resident of Bellevue, Pennsylvania, reported having lost \$50,000 worth of cryptocurrency sent to the Ethereum address 0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34 beginning in April of 20024 using a platform identifying itself as BIT and using the domain bwdcoin.cc. The description of the scam was consistent with pig butchering.
- f. MN, a resident of the Czech Republic, reported losing \$45,000 worth of cryptocurrency between April and September, 2024 after sending it to 0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34 using a site utilizing the domain bit-world.cc. The description of the scam was consistent with pig butchering.

50. Strike searched their records for other victims who sent BTC to the BIT-controlled Bitcoin addresses associated with RB's scam, and provided records identifying the following seven suspected victims who sent a total of 19.55870079 BTC (worth approximately \$1,173,647 at the time of the transactions) between June 28 and August 29, 2024, overlapping with the fraud against RB:

- a. Minneola, Florida resident GF sent a total of 2.95221562 BTC (worth approximately \$191,024) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV on June 28 and July 30, 2024. On September 5, GF reported to law enforcement that he was convinced by a person he met online to wire \$741,769 between September 18, 2023 and July 29, 2024 from his Chase Bank and Wells Fargo accounts to Coinbase, but he was now unable to withdraw and it appeared to be a “fake portal.” This description is consistent with a pig butchering scam.
- b. North Logan, Utah resident KD sent a total of 0.82139442 BTC (worth approximately \$48,950) to 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT on August 28 and 29, 2024. KD reported to law enforcement that he had lost at least \$200,000 between credit card transactions, wire transfers, and cryptocurrency transactions to the platform identifying itself as BIT and using the URL olurr.com. This URL is the same one used by RB.
- c. Jacksonville, FL resident AB sent a total of 2.37151095 BTC (worth approximately \$137,574) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV on July 31 and August 7, 2024. On September 12, AB reported to law enforcement that he had invested \$348,000 via Crypto.com in a supposed investment scam opportunity he was introduced to by someone he met in a chat room and corresponded with on WhatsApp. He reported the incident to law enforcement on September 12 after receiving a call from an FBI agent who warned he might be involved in a scam, and after his stockbroker told him they thought he was being scammed. This description is consistent with a pig butchering scam.
- d. U.S. resident RS sent a total of 0.61050823 BTC (worth approximately \$39,493) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV on July 16, 2024.
- e. U.S. resident DS sent a total of 3.28287845 BTC (worth approximately \$199,716) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV on August 9, 2024.
- f. U.S. resident JK sent a total of 0.21805695 BTC (worth approximately \$12,821) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV on August 12, 2024.
- g. U.S. resident JS sent a total of 6.60996847 BTC (worth approximately \$385,073) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV and 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT in five transactions between June 18 and August 30, 2024.

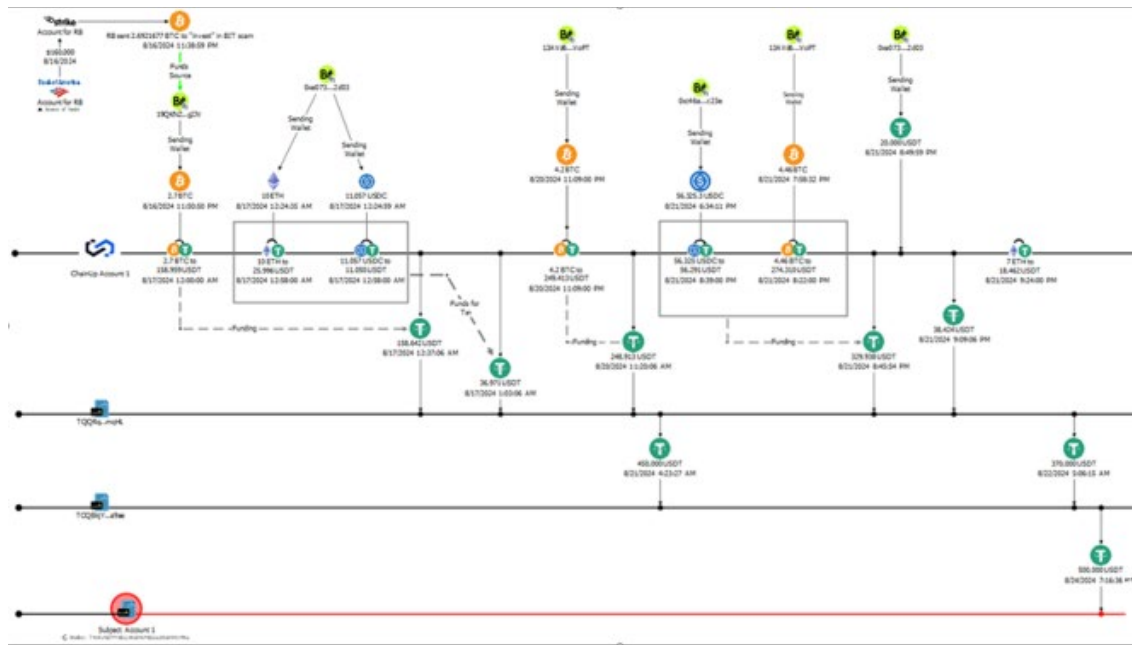
51. In total, the fourteen identified victims reported losses of approximately \$1,798,705.

Affidavit Name	City/State/Country	Loss	Address(es)
RB	Grass Valley, CA	\$167,000	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT 0xE073907d67A125DB8Fac7ea4719B3AaB94752D03 0xC46ABF247b6a0d86FF178561D0893ddD0f00C23e 0xE6626588bAea62C2229783D082d362c9525a1296 TJTWrPyts7ahu22iWupAfeGKDojqy9nLFF
WS	Lillington, NC	\$23,468	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
PT	Forsyth, GA	\$85,200	0x211d18f4262383911500e1298e02c4865e91abe2
TM	Roebuck, SC	\$2,000	Unknown
MW	Concord, SC	\$50,000	Unknown
RJ	Bellevue, PA	\$50,000	0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34
MN	Czech Republic	\$45,000	0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34
GF	Minneola, FL	\$191,024	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
KD	North Logan, UT	\$200,000	13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT
AB	Jacksonville, FL	\$348,000	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
RS	United States	\$39,403	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
DS	United States	\$199,716	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
JK	United States	\$12,821	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
JS	United States	\$385,073	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT
Total		\$1,798,705	

C. Facts Leading to the Identification of the Subject Accounts 1 and 2

52. As described below, I used the Blockchain to trace the victim's funds and commingled funds from BIT addresses through a series of transfers between cryptocurrency addresses, known as "hops," to their deposit at Subject Accounts 1 and 2. Once aware of the fraudulent conduct and tracing of victim funds, Tether Ltd., placed a voluntary freeze on the Target Property.

53. The illustration below shows the tracing of funds from RB's bank account to Subject Account 1:



54. The final withdrawal of RB's funds from Strike, sent as an intended investment to the Bitcoin address provided by BIT, occurred on August 16, 2024 in the amount of 2.6921677 BTC (approximately USD value \$158,996.20 at the time of the transaction) and was sent to the Bitcoin address 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV along with a small amount of additional BTC, for a total of 2.7 BTC. Approximately twelve minutes later, it was forwarded from that address to the address 1AD61wBMvt5DRPRV5mG6zAmpT91TGdDrqy in transaction ID 488651a91efb047c752c336834a2706ffc4fa56eb658bdb4e382099a673c7d68.

55. I have reviewed records from ChainUp, a cryptocurrency exchange, showing that this address is a ChainUp customer deposit address identified herein as "ChainUp Account 1." ChainUp records showed that approximately one minute after the 2.7 BTC was deposited into the account, the user of ChainUp Account 1 attempted to exchange that exact amount of BTC for USDT. The initial exchange was revoked, and a second attempt two minutes later successfully swapped the 2.7 BTC for 158,961.393 USDT. In my training and experience, I know that swaps

of this sort are often conducted with the intention of obfuscating the nature, source, ownership, control, and/or sources of funds.

56. 19 minutes after the swap from BTC to USDT, the account withdrew 158,642.4703 USDT on the Tron network to address TQQRqSbWvoQBDixpZpCUnW8PpZiAbWmqHL in Transaction ID 55fbfb4b296c84677aa125a9c5958598f101696139d71e7d189c98253141463c.

57. There were no other transactions within the account that occurred chronologically between the deposit of the BTC, the exchange for USDT, and the withdrawal of the USDT received from the exchange.

58. Prior to the TQQRqS... address receiving this input, there was only approximately 8,751 USDT in the address. The 158,642.4703 input was combined with two other inputs and three days later, 450,000 USDT (the entire balance except for approximately 3,278 USDT) was withdrawn to the address TCQBkjYHqx6HV2FG2PF2mWor2tULJTae. Before the 450,000 USDT was sent to the TCQBkj address..., that address had a USDT balance of zero. During approximately the following 27 hours, 50,000 USDT was withdrawn to a different address, another 370,000 USDT was received into the address, and then 500,000 USDT was sent to the address TNihvNZfFYdSjLWyEHIPXQ2u28oXHN1PNu, previously identified as Subject Account 1.

Voluntary Freeze of the Target Property by Tether Ltd.

59. Further analysis of the transaction history of the involved cryptocurrency addresses indicated that Subject Account 1 and another Tether address on the Tron network, TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF (previously identified as Subject Account 2), had a history of receiving inputs from addresses attributed to the BIT investment scam, after the

cryptocurrency had been moved in patterns consistent with the manner in which RB's funds were moved.

60. On September 4 and September 5, respectively, Tether placed a voluntary freeze on the USDT in Subject Accounts 1 and 2. At the time the accounts were frozen, the USDT balances in those accounts were 500,000 USDT and 900,000.145687 USDT, respectively.

Responses to the Freeze of the Target Property

61. Additional transaction activity occurred within Subject Accounts 1 and 2 after the addresses were "blocklisted" (frozen) by Tether Ltd.

62. In Subject Account 1, no other transaction activity had previously occurred other than the 500,000 USDT input. No TRX had ever been deposited into the account. TRX is the native currency of the Tron network and is necessary to pay the transaction fee for any withdrawal of USDT. On September 10, 2024 at 14:51:03 UTC, 70 TRX was deposited into the account. On that day at 14:51:45, a USDT transaction was attempted but failed, and a series of additional USDT transaction attempts followed. This behavior is consistent with the owner of the account attempting to withdraw USDT from the account and learning that withdrawals were being prevented.

63. Subject Account 2 had a more extensive transaction history with prior TRX inputs in the account. On September 10, 2024 at approximately 13:21:03 UTC (approximately 1.5 hours before the failed USDT transactions in Subject Account 1), a series of failed USDT transactions occurred in Subject Account 2. This behavior is consistent with the owner of the account attempting to withdraw USDT from the account and becoming aware that withdrawals were being blocked.

64. Tether Ltd. informed me that on September 11, 2024 an individual using the name “linda” contacted Tether from the email address linda11661166[.]gmail.com claiming ownership of both addresses in the Target Property.

65. I recognized the name “Linda” as the name used by the person who led RB to invest on the BIT platform.

66. On September 17, 2024 at 3:31 PM I received an email from linda11661166[.]gmail.com stating, “TNihvNZfFYdSjLWYEHIPXQ2u28oXHN1PNu This is my address and I would like to know how I can get my funds unfrozen and be able to transfer my assets normally, thank you.” The TNihvNZ... address is Subject Account 1.

67. Three minutes later I received an email from zjing6950[.]gmail.com stating, “TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF This is my address and I would like to know how I can get my funds unfrozen and be able to transfer my assets normally, thank you.” The TTscFq... address is Subject Account 2.

68. I noted that the language used in the two emails was identical, and the first email was sent from the email address that had initially claimed ownership of both addresses. Since then, I have received several emails from other email addresses claiming ownership of one or both of the Subject Accounts. I asked each requesting party to screen shot or take a video of them operating the wallet, to verify their ownership claim. One individual, using an email address different than those identified above, responded with a video that appeared to show a recording of a mobile phone with a Chinese language interface being used to access a wallet controlling Subject Account 2. On November 4, 2024, I replied to that user inquiring about their location to facilitate an in-person meeting. There was silence and no reply until December 24, when the user responded, claiming to be “from China and currently in Hong Kong” and asking to

remove the restrictions on the address. On December 31, I replied to that email and inquired about finding a mutually agreeable location to meet and discuss the origin of the funds. As of today's date, the user has not replied.

Post-Freeze Changes to the USDT Balances in Subject Accounts 1 and 2

69. Subject Account 1 received another deposit of 1.2 USDT on September 30, 2024.

70. Subject Account 2 received additional inputs of USDT on September 3 (254,015 USDT), September 8 (100,000 USDT), and September 10 at 19:39:42 UTC (100 USDT).

71. As of the writing of this affidavit, the USDT balances in these accounts are as follows:

a. 500,001.2 USDT in Subject Account 1

b. 1,000,100.145687 USDT in Subject Account 2

B. Laundering Fraud Proceeds Collectively to Subject Accounts 1 and 2

72. Using public blockchains and records obtained from cryptocurrency exchanges I used a "last in, first out" (or "LIFO") tracing methodology, in which the cryptocurrencies from immediately preceding transfers are the first withdrawn in subsequent transfers before any other funds, to examine the source of the USDT received by Subject Accounts 1 and 2.

73. The analysis focused on identifying the source all significant USDT deposits into the accounts (excluding *de minimis* amounts, specifically one deposit each of 1.20 USDT, 1.00001 USDT, and 100 USDT), including those USDT assets that remain frozen after other assets were withdrawn.

74. The analysis showed that various amounts of Bitcoin, Ether, USDT, and USDC cryptocurrency moved from the addresses attributed to BIT using some combination of multiple hops and decentralized swaps on the blockchain, rapid "pass-through" movement through

exchange accounts without converting to a different cryptocurrency or network, rapid “pass-through” movement through exchange accounts with conversion to a different cryptocurrency or network, the use of more than one exchange in sequence, re-aggregation after the movement through exchange accounts, and culminating in transfer to Subject Accounts 1 and 2.

75. During the course of the investigation I received records from the cryptocurrency exchanges ChainUp and 100ex pertaining to two involved ChainUp accounts and four involved 100ex accounts. Analysis of the account records indicated that the vast majority of funds received into at least five of these accounts were attributable to addresses attributed to the BIT scam. The customer due diligence records indicated that all of the account holders were from the People’s Republic of China, and the background of those photographs in which account holders were holding up their identification cards showed the photos were taken in what appeared to be the same corner of the same room, based on the shadowing and the coloration of the walls (see below). In two of the photos, what appears to be the same mark on the wall can be seen. The transaction patterns within the accounts were similar (deposits of BTC, ETH, USDC and USDT with most of the assets swapped to USDT on the Tron network). Withdrawals from both ChainUp accounts were nearly all to the same withdrawal addresses. Based on these facts, I believe at least three of the intermediary ChainUp and 100ex accounts were operated by the same organization and were used primarily for the laundering of the proceeds of cryptocurrency fraud.



ChainUp 1



ChainUp 2



100ex 3

76. Based on my training and experience, I know that criminals will often conduct an otherwise unnecessary number of transactions in the transfer of funds in an effort to layer ill-gotten funds to ultimately conceal or disguise the nature, location, source, ownership, or control of those proceeds when they are ultimately transferred into a cryptocurrency exchange. The number of hops and swaps involved is a strong indication that the movement of funds was performed in a manner meant to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity, to wit, wire fraud.

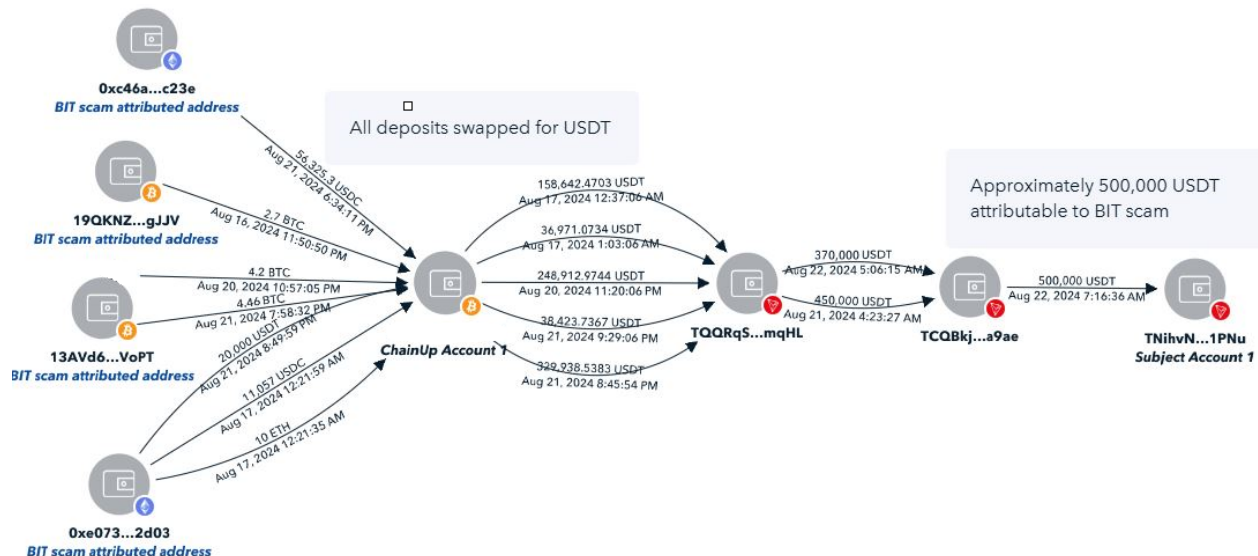
77. Based on the aforementioned LIFO principle, the undersigned calculated that in aggregate, approximately 100% of the total historical USDT inputs into Subject Account 1 (500,000 out of 500,001.2 USDT) and approximately 70% of the total historical USDT inputs into Subject Account 2 (approximately 1,788,453 out of 2,554,119 USDT) could be traced back to addresses attributed to the BIT scam and similar pig butchering scams.

78. Furthermore, also based on the aforementioned LIFO principle, the undersigned calculated that in aggregate, approximately 100% of the current, frozen balance of Subject Account 1 (500,000 out of 500,001.2 USDT) and conservatively no less than 26% of the current, frozen balance of Subject Account 2 (255,970 out of approximately 1,000,100 USDT),

representing in aggregate approximately 50% of the current balance of the two accounts, could be traced back to addresses attributed to the BIT scam and similar pig butchering scams based on the information currently available. The trackways of each significant input into Subject Accounts 1 and 2 are briefly summarized below.

Subject Account 1, Deposit Occurred 8/22/2024

79. A 500,000 USDT deposit into Subject Account 1 occurred on August 22, 2024 that originated in its entirety from addresses attributed to the BIT scam. The source of those assets is illustrated below. In summary, cryptocurrency assets in the form of USDT, USDC, ETH, and BTC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1, where they either passed through as USDT or were swapped for USDT. They were then withdrawn to TQQRqS..., where they were aggregated and forwarded to TCQBkj..., where they were further aggregated and then sent in a single deposit to Subject Account 1 after some of the funds in TCQBjk... were sent elsewhere.



Subject Account 2, Deposit Occurred 8/1/24 (Segment 1 of 2)

80. A 1,600,003 USDT deposit into Subject Account 2 occurred on August 1, 2024 that predominantly originated from addresses attributed to the BIT scam. There were two component inputs included in this deposit: one input of 300,003 USDT (segment 1 of 2), and another of 1,300,000 USDT (segment 2 of 2).

81. Segment 's sources are illustrated below. In summary, cryptocurrency (USDC, USDT, and BTC) was sent from BIT scammed addresses directly to ChainUp Account 1, where they were swapped for USDT. They were then withdrawn to TQQRqS..., where they were aggregated and forwarded to TRX82U..., where they were aggregated and forwarded to TG2YF4... after some assets were sent elsewhere, and then combined with segment 2 and forwarded to Subject Account 2.

82. The illustration below demonstrates the movement of these funds (segment 1 of 2) from attributed BIT scam addresses to Subject Account 2, of which approximately 300,000 USDT deposit is attributable to the BIT scam:

**Subject Account 2, Deposit Occurred 8/1/24 (Segment 2 of 2)**

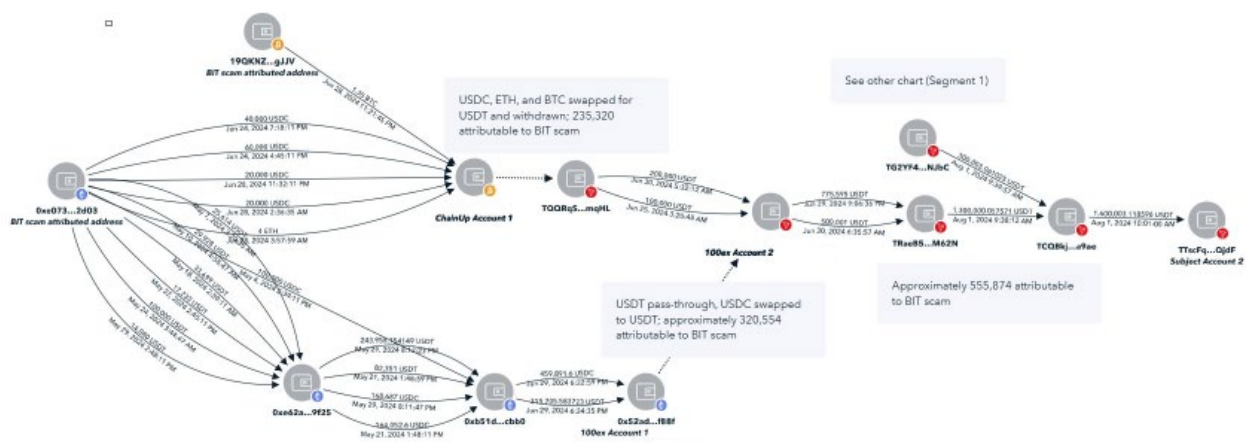
83. The 1,300,000 USDT segment of the 1,600,003 USDT deposit into Subject Account 2 that occurred on August 1, 2024 also originated in large part from addresses attributed to the BIT scam. The movement of funds occurred as follows, in summary:

- a. In one path, 100ex Account 1 received deposits of USDC and USDT indirectly (through either one or two hops) from an address attributed to the

BIT scam. 100ex Account 1 swapped the USDC for USDT, combined these deposits with other deposits, and transferred the USDT to 100ex Account 2, where approximately 320,554 USDT of the transferred assets were traceable to addresses attributed to the BIT scam. (See below for a description of the continued path from 100ex Account 2.)

- b. In a second path, cryptocurrency assets in the form of USDC, ETH, and BTC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1. There they were swapped for USDT and withdrawn to TQQRqS..., where they were aggregated and forwarded to 100ex Account 2, where approximately 235,320 USDT of the transferred assets were traceable to addresses attributed to the BIT scam. (See below for a description of the continued path from 100ex Account 2.)
- c. In two transactions on June 30, 2024, withdrawals 500,001 USDT and 775,595 USDT were made from 100ex Account 2 to TRaeB5..., of which approximately 555,874 USDT originated from addresses attributed to the BIT scam. These assets were forwarded from TRaeB5... where they were combined with other assets and forwarded to TCQBkj..., where they were aggregated with segment 1 and sent to Subject Account 2.

84. The illustrations below demonstrate the movement of these funds from attributed BIT scam addresses to Subject Account 2:

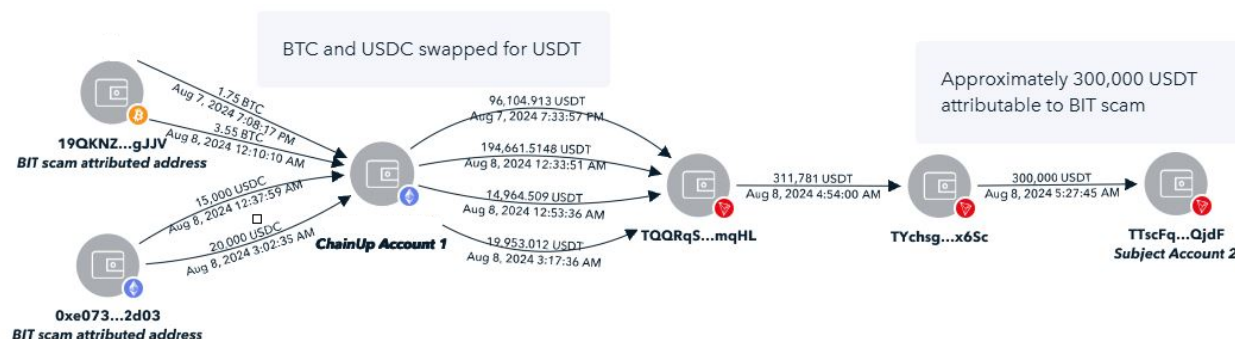


Subject Account 2, Deposit Occurred 8/8/24

85. A 300,000 USDT deposit into Subject Account 2 occurred on August 8, 2024 that originated in large part from addresses attributed to the BIT scam. In summary, cryptocurrency

assets in the form of BTC and USDC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1, where they were swapped for USDT. They were then withdrawn to TQQRqS..., where they were aggregated and forwarded in a single transaction to TYchsg..., from which some was sent to another destination and the remainder was forwarded to Subject Account 2. Approximately 300,000 USDT of that deposit was traceable to addresses attributed to the BIT scam.

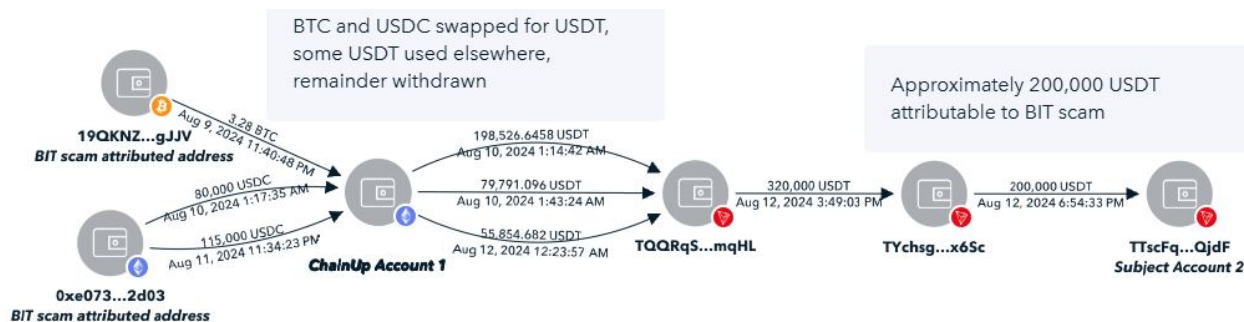
86. The illustration below demonstrates the movement of these funds from attributed BIT scam addresses to Subject Account 2:



Subject Account 2, Deposit Occurred 8/12/24

87. A 200,000 USDT deposit into Subject Account 2 occurred on August 12, 2024 that originated in large part from addresses attributed to the BIT scam. In summary, cryptocurrency assets in the form of BTC and USDC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1, where they were swapped for USDT. Some of the USDT was sent elsewhere and the balance was withdrawn to TQQRqS..., where they were aggregated and forwarded to TYchsg..., from which some was sent to another destination and the remainder was forwarded to Subject Account 2. Approximately 200,000 USDT of that deposit was traceable to addresses attributed to the BIT scam.

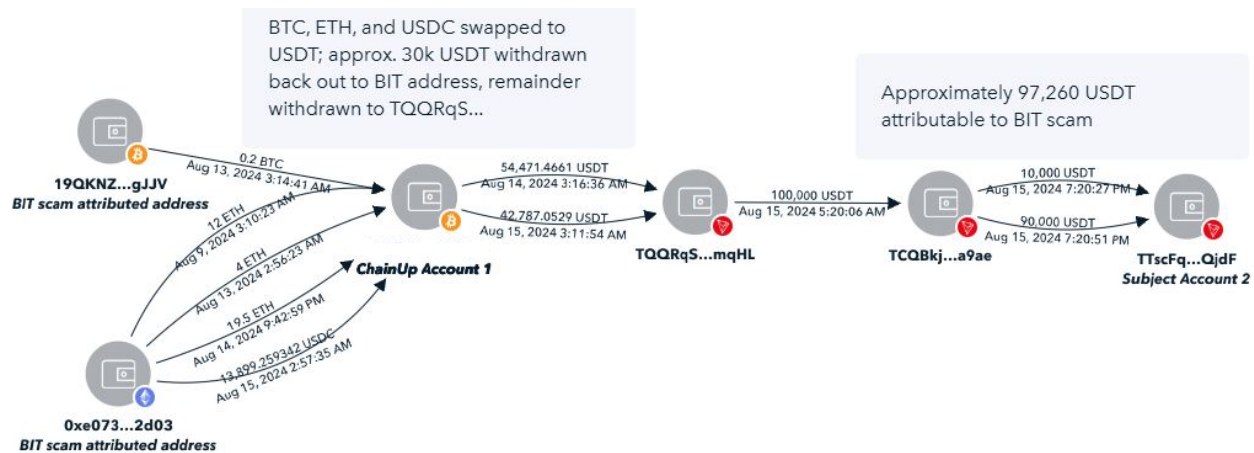
88. The illustration below demonstrates the movement of these funds from attributed BIT scam addresses to Subject Account 2:



Subject Account 2, Deposits Occurred 8/15/24

89. Two deposits of 10,000 and 90,000 USDT into Subject Account 2 occurred on August 15, 2024 that originated in large part from addresses attributed to the BIT scam. In summary, cryptocurrency assets in the form of ETH, BTC, and USDC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1, where they were swapped for USDT. They were then withdrawn to TQQRqS..., where they were aggregated and forwarded in a single transaction to TCQBkj..., from where they were sent in two deposits to Subject Account 2. Approximately 97,260 USDT of that deposit was traceable to addresses attributed to the BIT scam.

90. The illustration below demonstrates the movement of these funds from attributed BIT scam addresses to Subject Account 2:



Subject Account 2, Deposit Occurred 9/3/24

91. A deposit in the amount of 254,015 USDT occurred on 9/3/24 that originated in large part from addresses attributed to the BIT scam. In summary, cryptocurrency assets in the form of USDC and BTC were sent directly from addresses attributed to the BIT scam to 100ex Account 3, where they were swapped for USDT and then withdrawn to the TKdchh.... There they were combined and forwarded (along with additional USDT) to TCQBkj..., where they were combined with additional USDT and forwarded to Subject Account 2. Approximately 235,542 USDT of that deposit was traceable to addresses attributed to the BIT scam.

92. The illustration below demonstrates the movement of these funds from attributed BIT scam addresses to Subject Account 2:



Subject Account 2, Deposits Occurred 9/8/24

93. A deposit in the amount of 100,000 USDT occurred on 9/8/24 that originated in large part from addresses attributed to the BIT scam. In summary, cryptocurrency assets in the form of USDC were sent directly from an address attributed to the BIT scam to 100ex Account 3, where they were swapped for USDT and then withdrawn to the TKdchh... address. There they were combined and forwarded (along with additional USDT) to TTQ15w..., where some of the assets were combined with additional USDT and the balance was sent to Subject Account 2. Approximately 99,778 USDT of that deposit was traceable to addresses attributed to the BIT scam.

94. The illustration below demonstrates the movement of these funds from attributed BIT scam addresses to Subject Account 2:



C. GLEHFX.com Wire Fraud Scheme

95. During the course of this investigation another victim, a 38-year-old resident of San Jose referred to herein by his initials as “RM,” reported falling victim to a scheme with the following similarities to the BIT scheme targeting RB:

- a. RM was involved in the scam during the same period of time as RB;
- b. RM met an Asian woman online who claimed to be from another city on West Coast;
- c. The suspect corresponded with RM using some of the same communication applications used to communicate with RB;
- d. The suspect used the pretext of their relationship to introduce him to a speculative short-term trading opportunity utilizing cryptocurrency in which he interacted with a web site and a decentralized wallet application;

- e. The suspect claimed to be advised by an uncle who was a successful trader and led RM to believe that she had added funds to his account;
- f. RM funded the purported investments using cryptocurrency purchased on an exchange after being coached through the process of creating the exchange account and wiring funds from his bank accounts;
- g. RM was led to believe, through interaction with the app, that his investments had grown substantially in value; and,
- h. RM was led to believe that his account had been frozen and he had to pay an additional substantial fee to access his funds before he realized he was being defrauded.

96. RM's attempted investment in the GLEHFX platform is based on RM's statements and information viewable on public blockchains.

97. In or about June of 2024, RM connected with an individual named Chen YUE on Tinder. They began an online relationship and generally communicated on WhatsApp and Line. RM described YUE as an attractive Chinese female that spoke fair English but was not a native speaker. She appeared to be in an apartment and claimed that she was living in the hills of Los Angeles. RM was not provided any proof that she was actually in Los Angeles. RM said that sometimes their conversations had to end because what appeared to be a servant entered the room where she was video chatting.

98. In July of 2024, YUE encouraged RM to begin investing in an online App called Evjorerjrb, an Android-based app also associated with a web site GLEHFX.com. The application and webpage purport to make their users money through short-term leveraged short-selling gold contracts.

99. RM funded the gold trading account with payments of ETH. YUE guided him through the process of opening a Kraken account. RM funded his Kraken account with transfers from both his Bank of America account and his Wells Fargo account.

100. Prior to interacting with this website, RM had little knowledge and no experience in trading cryptocurrency. YUE said that she was being advised by a rich uncle who was successful in gold trading. RM was led to believe that YUE had also added \$85,000 into the account.

101. Between August 9 and 17, 2024, RM made four deposits from his Kraken account to the Evjorerjb/GLEHFX.com application totaling approximately 42.143 ETH, which at the time of the transactions had an approximate USD value of \$109,556. RM identified the transactions which investigators located on the Ethereum blockchain.

102. The online account made it appear as if their investment had made a \$480,000 profit in a matter of a few weeks.

103. After RM told YUE that he had no additional money to invest and that he wanted to withdraw funds, the website's account administrator informed RM on or about August 23, 2024 via an online message that he was being suspected of money laundering. He was requested to deposit an additional \$85,000 "to lift the account", and then the deposit would be returned to him.

104. RM became suspicious and began questioning YUE. He went to a residential address in San Jose that YUE had told RM that she owned as an investment, but the residents at that address had never heard of YUE. At that point RM realized he had been defrauded and reported the suspected crime to law enforcement.

Facts Leading to the Identification of Subject Account 3

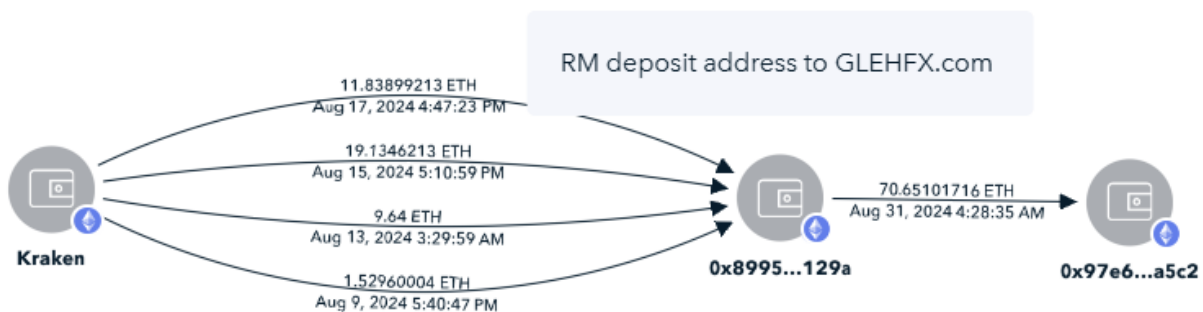
105. As described below, investigators traced the victim's funds and other funds from the addresses attributable to GLEHFX.com on the publicly available blockchain through a series

of transfers between cryptocurrency addresses, known as “hops,” to their arrival at Subject Account 3.

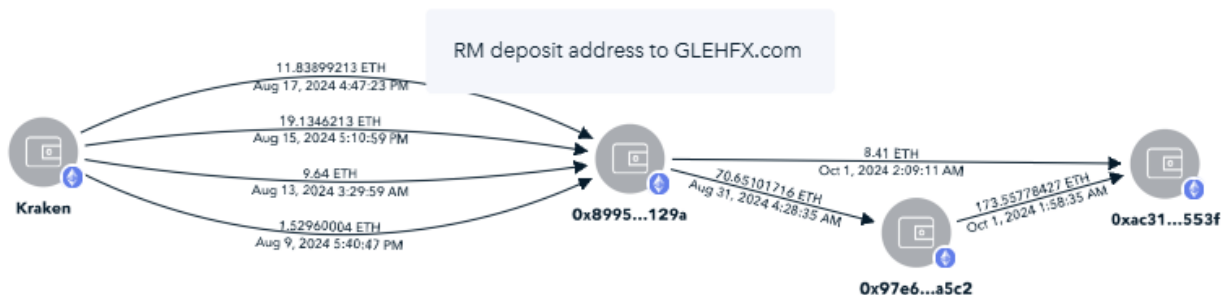
106. Investigators brought the account to the attention of Tether Ltd., which placed a voluntary freeze on Subject Account 3.

Laundering of the Proceeds of the Theft from RM and Discovery of Additional Victims

107. RM “invested” in the GLEHFX.com application by sending ETH from his Kraken account to the Ethereum address 0x899542876793412ba19D0b3265D01cea8F9E129a (which was provided to him by the scammers) in the transactions illustrated below, after which it was comingled with other funds and forwarded to the 0x97e6... address as illustrated below:



108. After the victim funds were sent to 0x97e6..., they were consolidated with other funds and sent to 0xaC319FBA26610b7685Cb2563D00Ef99f51A7553f. This address also had direct deposits from the address to which RM had sent his funds on October 1, 2024, as illustrated below:



109. Investigators located four additional reports made to iC3 establishing that the 0x97e6... address had received funds directly from victims involved in several similar Pig Butchering scams:

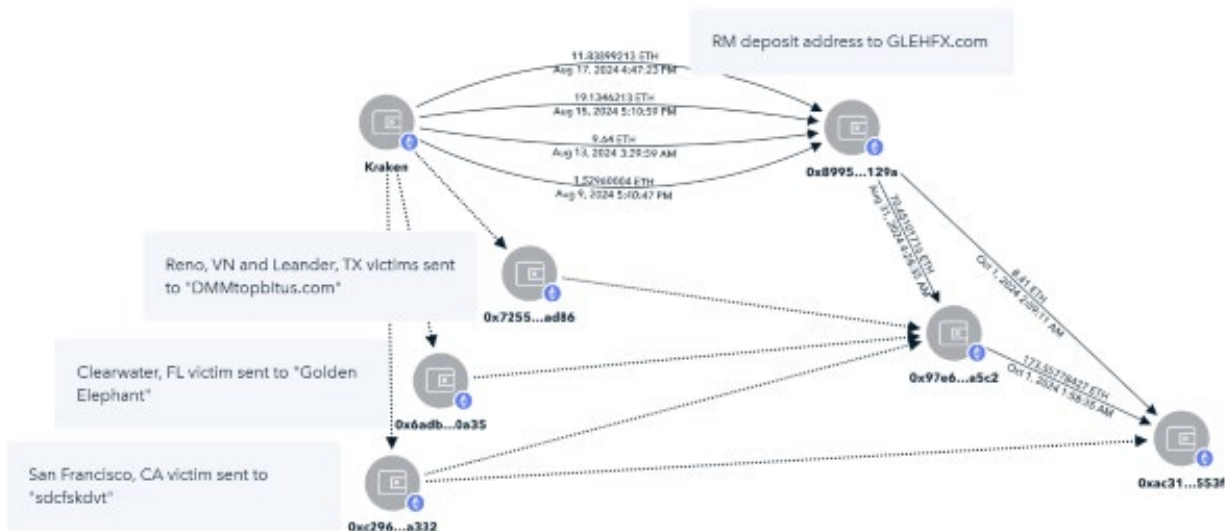
- a. A resident of Clearwater, Florida reported a loss of \$30,000 worth of cryptocurrency that occurred on or about May 13, 2024. The victim reported a woman he met online directed him in opening an account with a site called “Golden Elephant” to which he had sent approximately \$30,000 worth of cryptocurrency to the address 0x6ADb699b26e77F470a8F2bE0298957C4f2290A35. He was later unable to withdraw his funds and realized it was a scam.
- b. A resident of San Francisco, California reported a loss of \$25,000 worth of cryptocurrency that occurred on or about October 11 through 18, 2024. The victim reported that a woman he met through a wrong number call convinced him to invest cryptocurrency in a site accessed through an iPhone application called “sdcfskdvt.” At the suspect’s direction, he sent cryptocurrency to the address 0xc296E0E97b4E17d213df2BC044BE356C0499a332. He later realized it was a scam when he could not withdraw any funds and deposits that were purportedly made by the suspect to the victim’s account for his benefit did not appear on the blockchain.
- c. A resident of Reno, Nevada reported a loss of \$118,400 worth of cryptocurrency that occurred on or about March 19 and 20, 2024. The victim reported that he was befriended by a female met through a wrong number text message. She convinced him to take out a loan and invest through a web site using the URL DMMtopbitus.com. The victim sent the funds to the Ethereum address 0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86 at the direction of the suspect and learned it was a scam after he could not withdraw his funds and was asked to prepay “taxes.”
- d. A resident of Leander, Texas reported a loss of \$46,000 that occurred between approximately January 23 and February 7, 2024. The victim reported being befriended by a female met through a wrong number text message. She convinced the victim to invest in a website at the address DMMtopbitus.com, and he did so by depositing ETH to the address 0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86 and realized it was a scam after being asked to prepay his taxes.
- e. A resident of McDonough, Georgia reported a loss of \$133,580 that occurred on or about June 21, 2024. The victim reported having sent cryptocurrency to a fraudulent platform named DMM Bitcoin, at the direction of a friend he met through a messaging app. The victim was directed to send ETH to the address

0x1D95B2286cC4E8046bb868A1F20b2EC7CcafaB9F. The victim later realized this was a scam.

110. In total, these six identified victims reported losses of approximately \$462,536.

Affidavit Name	City/State/Country	Loss	Address(es)
RM	San Jose, CA	\$109,556	0x899542876793412ba19D0b3265D01cea8F9E129a
O-1	Clearwater, FL	\$30,000	0x6ADb699b26e77F470a8F2bE0298957C4f2290A35
O-2	San Francisco, CA	\$25,000	0xc296E0E97b4E17d213df2BC044BE356C0499a332
O-3	Reno, NV	\$118,400	0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86
O-4	Leander, TX	\$46,000	0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86
O-5	McDonough, GA	\$133,580	0x1D95B2286cC4E8046bb868A1F20b2EC7CcafaB9F
Total		\$462,536	

111. The proceeds of all these scams were forwarded to the 0xaC319FB address that had received RM's funds. That address had also received fund directly from the San Francisco victim described above. The paths of funds from the victims' exchange accounts to the 0xaC319FB... address are illustrated below.



112. On October 13, 2024, this consolidation address sent two deposits totaling approximately 292.8355 ETH to the address 0x366e2BEef3635b644D4698E33Ef557449ABeC8E7 ("Subject Account 3"). This address had

been funded solely by these two transactions. On November 18, 2024, approximately 92 ETH was sent in two transactions to a decentralized finance application and converted within the same address to approximately 285,157.35 USDT.

113. On November 18, 2024, investigators brought the suspected illicit activity to the attention of Tether Ltd. At that time the USDT balance in Subject Account 3 was approximately 281,158 USDT.

Voluntary Freeze of Subject Account 3 by Tether Ltd., and Subsequent Account Activity

114. On November 20, 2024, Tether placed a voluntary freeze on the USDT in Subject Account 3.

115. By the time the account was “blocklisted” (frozen), two withdrawals of USDT had been conducted, leaving a USDT balance of only 0.547356 USDT.

116. As noted, the Ethereum address containing that remaining USDT had been used to swap ETH for USDT using decentralized finance applications. That address still contained a substantial amount of ETH attributable to the identified scam deposit addresses. As a result, the account remained voluntarily blocklisted by Tether. This blocklisting allowed new deposits of USDT, but not withdrawals, to occur.

117. On December 1, 2024, Subject Account 3 sent 348.8 ETH to a decentralized finance application and received 1,285,539.809879 USDT in exchange. The freeze placed by Tether Ltd. remains in place.

118. On December 26, 2024, Tether Ltd. informed investigators that they had been contacted by someone claiming ownership of Subject Account 3 who provided only the name “rui” and the email address from the domain 163.com. Tether provided them with contact information for a REACT investigator but no contact has been received from that individual.

119. As of the writing of this affidavit, the USDT balances in Subject Account 3 is 1,285,540.357235.

B. Laundering Fraud Proceeds Collectively to the Target Property

120. Using public blockchains and records obtained from cryptocurrency exchanges I used the aforementioned LIFO tracing methodology to examine the source of the USDT received by Subject Account 3.

121. All of the USDT ever received by Subject Account 3 was derived from ETH deposits into the account, whereby the ETH deposited into the account was swapped within the account for USDT using a decentralized finance application.

122. There were three deposits of ETH into the account:

- a. A deposit of 0.1 ETH on October 13, 2024
- b. A deposit of 292.735563 ETH on October 13, 2024
- c. A deposit of 147.588713 ETH on November 28, 2024.

123. The analysis focused on identifying the source these ETH deposits.

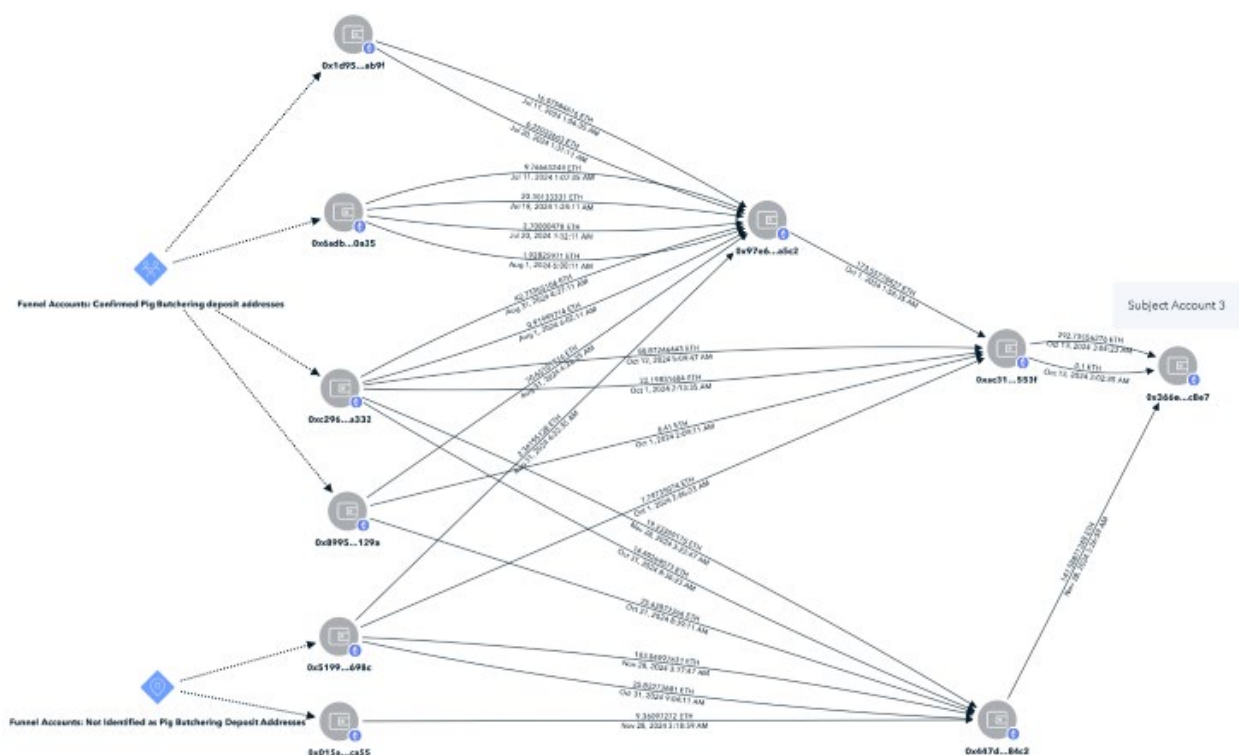
124. All of the ETH inputs received by Subject Account 3 arrived via six “funnel accounts,” which collected ETH from a variety of sources and forwarded it via either one or two “hops” to Subject Account 3.

125. Based on the information currently available, four of those six “funnel accounts” have been identified by victim reporting as scam deposit addresses, as described above.

126. Based on my training and experience, I know that criminals will often conduct an otherwise unnecessary number of transactions in the transfer of funds in an effort to layer ill-gotten funds to ultimately conceal or disguise the nature, location, source, ownership, or control of those proceeds when they are ultimately transferred into a cryptocurrency exchange. The

aggregation of illicit funds in “funnel accounts” and the forwarding of the funds through one or more hops to an aggregation address where the funds are swapped for another type of cryptocurrency is an indication that the movement of funds was performed in a manner meant to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity, to wit, wire fraud.

127. The paths of the inputs into Subject Account 3 from the “funnel accounts” are illustrated below:



128. Based on the aforementioned LIFO principle, the undersigned calculated that in aggregate, at least approximately 72% of the total historical ETH inputs into Subject Account 3 (317.9645 of the total 440.3243 ETH received), and therefore 72% of the total historical USDT inputs into the account, could be traced back to addresses attributed to Pig Butchering scams.

129. Furthermore, also based on the aforementioned LIFO principle, the undersigned calculated that in aggregate, conservatively no less than approximately 51% of the current,

frozen balance of Subject Account 3 (approximately 659,710 out of 1,285,540 USDT) could be traced back to addresses attributed to Pig Butchering scams based on the information currently available.

SEIZURE PROCEDURE FOR THE TARGET PROPERTY

130. There is probable cause to believe the funds held in the Target Property are subject to civil and criminal forfeiture, as proceeds of wire fraud and involved in illegal money laundering.

131. Law enforcement intends to work with Tether to seize the funds associated with the Target Property. In sum, the accompanying warrants would be transmitted to Tether, and Tether will “burn” (*i.e.*, destroy) the addresses at issue (and by extension the USDT tokens associated with them). Tether would then reissue the equivalent amount of USDT tokens associated with the Target Property and transfer that equivalent amount of USDT to a government-controlled wallet. The seized currency will remain in the custody of the U.S. government during the entire pendency of the forfeiture proceedings, to ensure that access to, or manipulation of, the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

CONCLUSION

132. Based on information derived from the foregoing investigation, there is probable cause to conclude that the Target Property contains the proceeds of a wire fraud scheme performed in violation of Title 18, United States Code, Section 1343. Those proceeds, which include 1,415,680 USDT from the Target Property, are subject to seizure and forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section

2461(c). Moreover, there is probable cause to believe that the proceeds of other schemes, Pig Butchering or otherwise, are also present in the Target Property. Finally, there is further probable cause to believe that a greater amount of funds constitute property involved in money laundering transactions, to wit: the entire USDT balance of the Target Property. These funds are accordingly subject to forfeiture and seizure pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1). Accordingly, I respectfully request that warrants be issued authorizing the seizure of the Target Property with the goal of returning these funds to the victims impacted by the various scams implicated in this investigation.

133. I submit that a protective or restraining order issued pursuant to 21 U.S.C. § 853(e) would be insufficient to ensure the availability of the funds in the Target Property for forfeiture. Cryptocurrency can be transferred faster than traditional bank funds, and once transferred, generally cannot be recalled to an original wallet. Moreover, there is a risk that the funds may be moved to a location where no forfeiture or seizure would be possible, at which point the funds could be further laundered into a “privacy” (i.e. untraceable) cryptocurrency. Thus, I submit that seizure warrants are the only means to reasonably assure the availability of the funds in the Target Property for forfeiture.

134. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Respectfully submitted,



DAVID BERRY
Criminal Investigator, Santa Clara County
Office of the District Attorney
Special Deputy U.S. Marshal,
U.S. Secret Service Cyber Fraud Task Force

Reviewed and approved as to form

/s/ Kevin C. Khasigian
Kevin C. Khasigian
Assistant U.S. Attorney

Sworn before me and signed
telephonically on this 13th day of
January 2025 at 5:52 PM.

/s/
Hon. Carolyn K. Delaney
United States Magistrate Judge

ATTACHMENT A: PROPERTY TO BE SEIZED

Pursuant to this warrant, Tether shall provide the law enforcement officer/agency serving this document with the equivalent amount of USDT tokens that are currently associated with the virtual currency addresses referenced below (*i.e.*, 2,785,641.702922 USDT). Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency addresses referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency wallet. Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

- 500,001.2 USDT held in the Tron account
TNihvNZfFYdSjLWyEHIPXQ2u28oXHN1PNu
- 1,000,100.145687 USDT held in the Tron account
TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF
- 1,285,540.357235 USDT held in the Ethereum account
0x366e2beef3635b644d4698e33ef557449abec8e7

United States District Court

EASTERN District of CALIFORNIA

In the Matter of the Seizure of
(Briefly describe the property to be seized)

1,285,540.357235 USDT held in the Ethereum account
0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7.

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

CASE NUMBER:

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the BRITISH VIRGIN ISLANDS be seized as being subject to forfeiture to the United States of America. The property is described as follows:

**1,285,540.357235 USDT held in the Ethereum account
0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7.**

The property is subject to seizure pursuant to 18 U.S.C. §§ 981(b) and 982(b), and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), and 982(a)(1), and 28 U.S.C. § 2461(c).

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property within 14 days in the daytime 6:00 a.m. to 10:00 p.m. You must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to CAROLYN K. DELANEY or Any U.S. Magistrate Judge in the Eastern District of California.

January 13, 2025 at 5:52 PM

/s/

Date and Time Issued

Judge's signature

Sacramento, California
City and State

Carolyn K. Delaney, U.S. Magistrate Judge
Printed name and title

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture (Page 2)

RETURN

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken:

CERTIFICATION

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

Subscribed, sworn to telephonically, and returned before me this date.

U.S. Judge or Magistrate_____
Date

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEIZURE WARRANTS**

I, David Berry, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND PURPOSE OF AFFIDAVIT

1. I submit this affidavit in support of an application for the issuance of three seizure warrants for cryptocurrency assets held in two Tether accounts on the Tron network and one Tether account on the Ethereum network, collectively referred to hereinafter as the “Target Property,” to wit:

- a. 500,001.2 USDT held in the Tron account
TNihvNZfFYdSjLWyEHIPXQ2u28oXHN1PNu, hereinafter referred to as
“Subject Account 1,” and;
- b. 1,000,100.145687 USDT held in the Tron account
TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF, herein referred to as “Subject
Account 2,” and
- c. 1,285,540.357235 USDT held in the Ethereum
account0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7, herein
referred to as “Subject Account 3.”

2. The property to be seized and the seizure procedure is described in the following paragraphs and in Attachment A.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that unknown subjects have violated Title 18, United States Code, § 1343 (Wire Fraud) and laundered the proceeds of that activity in violation of Title 18, United States Code, § 1956(a)(1)(B)(i) (Money Laundering). There is also probable cause to believe that the Target Property contains the proceeds of the wire fraud scheme described below. Accordingly, the fraud and money laundering proceeds, totaling approximately 1,415,680 USDT are subject to seizure and forfeiture pursuant to Title 18, United States Code, § 981(a)(1)(C), and Title 28, United States Code, § 2461(c). Moreover, as indicated herein, there is probable cause to

believe that the Target Property has been used to launder the funds of criminal activity.

Accordingly, there is also probable cause to seize the Target Property as funds involved in money laundering transactions, pursuant to Title 18, United States Code, §§ 981(a)(1)(A) and 982(a)(1).

4. The facts in this affidavit come from my personal observations and knowledge, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. All dates are on or about the date specified. All amounts are approximate.

5. I accordingly request that the Court authorize the attached warrants for seizure of the assets described herein.

AGENT BACKGROUND

6. I am an “investigative or law enforcement officer” of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am a Special Deputy United States Marshal, sponsored by the United States Secret Service, and empowered by law to conduct criminal investigations and make arrests for offenses enumerated in Title 18 of the United States Code.

7. I am currently employed as a Criminal Investigator with the Santa Clara County Office of the District Attorney and have been so employed since December 2012. Since August 2015 I have been assigned to the Regional Enforcement Allied Computer Team (“REACT”) Task Force, where my primary duties include the investigation of technology-related crimes with an emphasis on cyber-facilitated fraud and theft. I attended the Peace Officer Standards and Training (“POST”) Basic Police Academy in San Jose, California in 2003, where I received formal training in the investigation of a variety of crimes. I have been a sworn peace officer

since 2003, during which time I have participated in hundreds of criminal investigations involving various types of computer crimes. I have earned a certificate in the Investigation of Computer Crimes from the Robert Presley Institute of Criminal Investigations. From March through September 2017, I participated in a full-time fellowship with the FBI's National Cyber Investigative Joint Task Force, where I worked with various United States Government organizations to obtain additional training and experience in conducting technology-related investigations, including those involving cryptocurrency. I have also attended numerous other courses during which I received training in the investigation of technology-related crimes and the collection of digital evidence for use in criminal investigations. I have taken several formal training courses regarding cryptocurrency and its application to criminal investigations, have conducted dozens of investigations involving the criminal use of cryptocurrency, and have taught classes on this topic to other law enforcement investigators throughout the United States on numerous occasions. I have investigated dozens of cases of cryptocurrency theft, including many involving fraud schemes like the one described herein. I have been recognized as an expert in Santa Clara County Superior Court on the subjects of cryptocurrency investigation and the fraud scheme described herein.

8. Title 18, United States Code, Sections 981(b)(2) and (3) provide that seizure warrants shall be made pursuant to a warrant issued in the same manner as provided for a criminal search warrant under the Federal Rules of Criminal Procedure. Moreover, seizure warrants may be issued in any district in which a forfeiture action may be filed and may be executed in any district in which the property is found. Federal Rule of Criminal Procedure 41 governs the issuance of criminal search and seizure warrants.

9. Title 28, United States Code, Section 2461(c) provides that the procedures (including seizure warrants) in Title 21, United States Code, Section 853 control criminal forfeiture. Section 853(f) of the same title provides that the government may request a warrant for the seizure of property for forfeiture in the same manner as it may seek a search warrant. Title 18, United States Code, Section 982(b)(1) also provides that seizures for criminal forfeiture shall be made pursuant to a warrant issued in the same manner as provided for a criminal search warrant under the Federal Rules of Criminal Procedure, and cross-references Title 21, United States Code, Section 853. This warrant seeks seizure authority under both the criminal and civil forfeiture statutes.

10. Title 21, United States Code Section 853(f) provides that a court may issue a criminal seizure warrant when it “determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a[] [protective] order under [21 U.S.C. § 853(e)] may not be sufficient to assure the availability of the property for forfeiture.” As set forth further below, there is a substantial risk that the Target Property will be withdrawn, moved, dissipated, or otherwise become unavailable for forfeiture unless immediate steps are taken to secure them. I therefore submit that a protective order under 21 U.S.C. § 853(e) would not be sufficient to assure that the Target Property will remain available for forfeiture.

11. One of the chief goals of forfeiture is to remove the profit from crime by separating the criminal from his or her dishonest gains, and to divest criminal actors from the apparatus allowing them to engage in criminal activity. *See United States v. Newman*, 659 F.3d 1235, 1242 (9th Cir. 2011); *United States v. Casey*, 444 F.3d 1071, 1073 (9th Cir. 2006). To that end, in cases involving a money laundering offense, the forfeiture statutes connected to money

laundering offenses permit the government to forfeit property “involved in” money laundering. Such property includes “untainted property” commingled with “tainted” property, when that untainted property is used to facilitate the laundering offense, such as by obscuring the nature, source, location, or control of any criminally derived property. *See* Title 18, United States Code, Sections 981(a)(1)(A), 982(a)(1); *see also United States v. Kivanc*, 714 F.3d 782, 794-95 (4th Cir. 2013); *United States v. Huber*, 404 F.3d 1047, 1056-1058 (8th Cir. 2005).

12. Based on my training, experience, and the information contained in this affidavit, there is probable cause to believe that funds in the Target Property are subject to both civil and criminal forfeiture as proceeds traceable to a wire fraud scheme, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c). The balance of the Target Property is subject to both civil and criminal forfeiture as property involved in money laundering, pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1). The balances of the virtual currencies in the Target Property are therefore subject to civil and criminal seizure.

CRYPTOCURRENCY AND VIRTUAL CURRENCY EXCHANGES

13. Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar but are generated and controlled through computer software. Bitcoin is currently the most well-known virtual currency in use.

14. Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters.

15. Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password needed to access the

address. An address is somewhat analogous to a bank account number and is represented as a string of letters and numbers up to 40 characters long. Users can operate multiple addresses at any given time, with the possibility of using a unique address for every transaction. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address. Although the identity of an address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity.

16. A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

17. Many virtual currencies publicly record all of their transactions on what is known as a "blockchain." The blockchain is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

18. **Stablecoins**: Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDC and USDT are stablecoins pegged to the U.S. dollar.

Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

19. **Tether (USDT):** Tether Limited (“Tether”) is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USD Tether (“USDT”) tokens. USDT is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a “stablecoin.” USDT is hosted on the Tron and Ethereum blockchains, among others.

20. **Tron (TRX):** Tron (“TRX”) is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses smart contract technology. The public ledger is the digital trail of the Tron blockchain, which allows anyone to track the movement of TRX and tokens such as USDT.

21. **Ether (ETH) and Ethereum:** Ether (“ETH”) is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a network called Ethereum that uses smart contract technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH and tokens such as USDT.

22. **USD Coin (USDC):** USD Coin (“USDC”) is a blockchain-based a stablecoin. USDC is hosted on the Ethereum network, among others. USDC is issued by Centre, a company headquartered in the U.S. USDC is connected to Coinbase and Circle, cryptocurrency exchanges registered in the U.S.

23. **Smart contracts:** Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract’s code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using blockchain protocols such as Ethereum and Tron to maintain

transparency. Multiple cryptocurrencies, including USDT, can utilize the Ethereum or Tron blockchains to take advantage of this technology. Smart contract technology is one of the distinguishing characteristics of Ethereum and Tron and is an important tool for companies or individuals executing trades on these blockchains. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum or Tron blockchain and is both trackable and irreversible.

24. **Decentralized finance application:** One of the many applications of smart contracts on blockchains such as Ethereum is to facilitate financial transactions involving cryptocurrency that do not rely on a centralized custodial service to execute. Such applications are decentralized in nature as they rely on pre-established smart contracts (rather than trusted intermediaries) to execute code automatically in response to certain inputs. These applications are commonly used to “swap,” for example, Ethereum for USDT, or USDT for another Ethereum token, such that one asset is sent from the address and an equivalent value (less fees) of the corresponding asset is received into the same address nearly instantaneously, within the same transaction. Services utilizing these mechanisms are often referred to as “decentralized finance applications.”

PROBABLE CAUSE

25. This investigation was initiated from a fraud report received by the REACT Task Force, a participating member of the USSS San Francisco Field Office’s Cyber Fraud Task Force, from “RB”, a 62-year-old resident of Grass Valley, California, in the Eastern District of California. In or about June through August of 2024, RB fell victim to an ascending investment

fraud scheme known as “Pig Butchering”, which resulted in a total loss of approximately \$167,000 to RB.

26. The investment scam detailed in this affidavit is consistent with Pig Butchering scams in general. Pig Butchering originated in China in 2019 and often begins with a perpetrator sending a victim an unsolicited text message, typically via WhatsApp or a social media/dating website. From the initial message, the perpetrator develops an intimate relationship with the victim using manipulative tactics similar to those used in online romance scams. Pig Butchering schemes frequently originate in various locations throughout Southeast Asia, including, but not limited to, Hong Kong, Myanmar, Cambodia, Malaysia, Thailand, and Singapore.

27. Pig Butchering victims are referred to as “pigs” by the perpetrators, because the perpetrators will use elaborate (and often romantic) storylines to “fatten up” victims into believing they are in a trusting relationship. Once the victim reaches a certain point of trust, they are brought into a cryptocurrency investment scheme and provided fabricated evidence to bolster the scheme’s legitimacy and eliminate any skepticism the victim may have about the investment (i.e., the ongoing scam). Victims are provided fake investment platforms via a website or mobile application that showcases fictitious investment gains. In reality, the website or application has limited functionality and does not provide the user any access to a cryptocurrency wallet. The perpetrators may also provide fake transaction photos to create the false impression the perpetrators are contributing their own funds to the victim’s initial investment. However, the investment gains displayed on the investment platform website or mobile application are fabricated. In truth, the investment platform does not exist.

28. The perpetrator encourages victims to invest more funds into the platform, with the promise of higher returns. Victims are often allowed to make small initial withdrawals to

bolster the perception of control over the assets, as part of the effort to increase trust in the platform and encourage larger investments. When significant withdrawals are attempted, however, they are not allowed. Various excuses are given for blocked withdrawals, often involving fees and taxes that are due (and require "fresh money" rather than being paid from supposed gains) and sometimes alleging that suspected misconduct has caused a freeze of the account for compliance purposes. Victims are ultimately unable to withdraw their funds regardless of how much more money is contributed to the platform, and their investment funds are stolen from them. The financial loss causes the victims financial, personal, and emotional ruin and is referred to by the perpetrators as “butchering” or “slaughtering” the victims.

29. The efforts to defraud RB were evident within approximately two weeks of the perpetrator’s initial message on Facebook, as RB purchased USDT, USDC and Bitcoin from cryptocurrency exchanges Crypto.com and Strike and transferred it into the fraudulent trading application, “BIT.”

30. The “BIT” application used to defraud RP appears to be a play on the legitimate cryptocurrency trading business with the same acronym, “BIT”. The acronym “BIT” used hereafter refers to the fraudulent platform, not the legitimate company that was not involved in this caper.

31. The fake BIT platform gave the illusion that RP had huge gains from high-frequency trading. However, the perpetrator offered various excuses—and even demanded more money—when RB tried to withdraw funds. RB contributed a net total of approximately \$165,000 worth of cryptocurrency to the investment scheme before realizing it was a scam.

A. “BIT” Impersonation Wire Fraud Scheme

32. The summary of RB's investment in the BIT platform is based on RB's statements, screen shots provided by RB of his interactions with the perpetrators and the bogus investment platform, records obtained from the cryptocurrency exchange Strike pertaining to RB's account, and information viewable on public blockchains.

33. In or about June of 2024, RB was participating in a motorcycle enthusiast Facebook group when he was messaged by a female identified as "Linda GAO." GAO claimed to own a motorcycle and they chatted a few times on Facebook, including video chats. After a matter of days, GAO asked that they move the chat to WhatsApp.

34. RB later noticed that some of the wording was strange, so he asked if GAO was using a translator, and GAO confirmed she was. In retrospect, RB thinks he likely chatted with different people at different times based on the changing personalities he encountered chatting with GAO.

35. Based on my knowledge and experience conducting cryptocurrency fraud investigations, I know that these criminal organizations often operate in multiple tiers of responsibility. Most often, the individual that communicates directly with the victim is on a lower tier of responsibility in the criminal organization, whereas individuals receiving funds at the end of the scheme are those who profit the most and are typically higher in the criminal organization's hierarchy.

36. Based on my knowledge and experience in investigating cyber fraud schemes, GAO is most likely not the person portrayed to the victim during their WhatsApp conversations and may actually be a role played by multiple individuals. After a week or so, the conversation with GAO shifted to money. GAO claimed to have a degree in economics and started talking about cryptocurrency. GAO told RB she had made a lot of money trading cryptocurrency options

and offered to help RB make money doing the same. RB confided in GAO that his father had dementia and he needed money to pay for his father's care.

37. At GAO's direction, RB downloaded the TrustWallet cryptocurrency wallet application to his mobile device and used it to connect to a platform called "BIT" accessed via a URL provided by GAO. He created an account on the BIT platform which he always accessed via TrustWallet. Based on my training and experience, I know that perpetrators of Pig Butchering scams provide links to applications and website that function and appear like legitimate cryptocurrency platforms. The apps and sites display information that include account numbers, cryptocurrency wallet addresses, investment amounts and gains, and deposit/withdrawal functions. The application featured graphics and layouts consistent with most extant smartphone currency trading applications. The perpetrators routinely adjust the displays as they see fit through the course of the scam.

38. The site's URL often changed, approximately monthly. The site's initial URL was <https://cntzcy.com>. On July 30, 2024, RB received an email from the platform's customer service email stating that due to a "hacked malicious attack," the web platform's domain changed to <https://cdsslt.com>. On August 28, 2024, RB received an email from the platform customer service email stating that the platform's web domain had changed to <https://oluarr.com>, again due to another "hacked malicious attack."

39. Based on my training and experience, I know it is common for perpetrators to change the domain names of the web sites where their bogus site is hosted in order to maintain continuity of operations when victim reporting leads to the initial domain being identified online as fraudulent, or blocked or taken down by webhost providers, registrars, or government authorities. In addition, it would be unusual and counterproductive behavior for a legitimate

business to frequently change its web address, or to use such different URLs that appear to have no relationship to the actual name of the company or service.

40. GAO showed him how to use BIT and explained that there were different tiers of investment, where the expected rate of return from investing in different pools of options (for example the 30-second pool, 60-second pool, or 90-second pool) increased with the amount of money invested. By investing more, higher rates of return could be achieved.

41. RB sent some cryptocurrency from his preexisting account at the exchange Crypto.com to BIT, using the deposit address provided to him by BIT. The cryptocurrency was purchased using credit cards linked to his Crypto.com account and wire transfers from his Bank of America account. Between July 14 and July 21, 2024, RB sent at least 38,150 USDC from his Crypto.com account to his own unhosted wallet, and from there to the address provided by BIT to deposit the assets into his BIT account.

42. RB experienced disruptions with the Crypto.com transactions and told GAO, who urged RB to instead use the Strike exchange to avoid the barriers created by Crypto.com. GAO guided RB through the transition to Strike, and RB registered an account at Strike for the purpose of investing in BIT.

43. On or about July 25, 2024, RB sent \$5,000 from his Bank of America account to his Strike account. RB purchased \$5k worth of BTC and sent it to the address provided by BIT to make a deposit into his account. At one point, after sending funds from Crypto.com and Strike, RB had a \$60k balance of his own funds in the BIT account. On or about August 13, 2024, RB successfully withdrew those funds from his BIT account to his Strike account and then withdrew \$59,716.60 from his Strike account to his Bank of America account. This experience convinced

RB that GAO's investment opportunity was sincere and legitimate, because RB believed if they were going to steal his \$60k, they would have kept it.

44. GAO offered to loan RB \$50k to propel him into a higher tier of return on BIT, and when RB agreed to the arrangement, RB's funded balance on BIT showed a \$50k increase of cryptocurrency. GAO later purportedly added another \$150k worth of loans to RB's account, as reflected in his BIT balance. The cryptocurrency GAO transferred to RB appeared as if it had been transferred from Crypto.com. GAO told RB that a big trade opportunity was forthcoming but would only be open for a short period because of increased risk factors connected to election politics. GAO ultimately convinced RB that he needed another \$160k to step up into the next tier. Between GAO's supposed loans to RB, the funds RB personally invested, and the purported investment gains, RB's account reflected a sufficient balance to reach the next tier.

45. On or about August 16, 2024, RB wired \$160,000 from his Bank of America account to his Strike account. RB used the \$160,000 in his Strike account to purchase 2.69292824 BTC, which RB sent to his BIT account (to an address provided by BIT). By August 27, 2024, his account on BIT appeared as if he had over \$924,000 worth of USDT. GAO told him that trades would be paused for a while because of political turmoil surrounding the election, and suggested he cash out.

46. In mid to late August, RB requested a withdrawal of approximately 674,000 USDT from BIT, but BIT showed that the withdrawal was "pending clearance" or "on hold." The next morning, on or about August 21, 2024, BIT's message changed to "Contact customer service" and indicated RB's account was locked because RB had input the wrong receiving address. However, RB compared screen shots he entered and confirmed he had input the correct address. BIT's message now showed a missing digit.

47. RB contacted BIT's online service assistant who advised RB to deposit 20% of his balance (approximately \$180,000) to unfreeze the funds. If RB did not comply and deposit more funds within three days, the balance of his account would be donated to the United Way. At this point, RB concluded that the investment was a scam and contacted law enforcement.

B. Cryptocurrency Addresses and More Victims of the BIT Scam

48. During the investment scam, BIT provided instructions to RB to transfer funds to a series of cryptocurrency addresses, which are reproduced below:

- a. The Bitcoin addresses 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV, 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT, and bc1qjh6dc0scfu9vdyf2yjdjhj96uvlvtf6tdhhw8ml were provided for BTC deposits. His largest and final deposit of 2.6921677 BTC was sent to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV and was reflected in his BIT account balance. This address was also the source of the BTC withdrawals he successfully received from BIT.
- b. The Ethereum address 0xE073907d67A125DB8Fac7ea4719B3AaB94752D03 was provided for USDC deposits. RB made two USDC deposits to this address that were reflected in his BIT account balances.
- c. The Ethereum address 0xC46ABF247b6a0d86FF178561D0893ddD0f00C23e was provided for both USDT and USDC deposits. RB did not make actual deposits to this address.
- d. The Ethereum address 0xE6626588bAea62C2229783D082d362c9525a1296 was provided for USDT deposits. RB did not make actual deposits to this address.
- e. The Tron address TJTWrPyts7ahu22iWupAfeGKDojqy9nLFF was provided for USDT deposits on the Tron network. RB did not make actual deposits to this address.

49. I connected the above addresses to other related victim complaints on the Federal Bureau of Investigation's ("FBI's") Internet Crime Complaint Center, known as IC3 (<http://www.ic3.gov>). The following seven IC3 reports, also victims of purported Pig Butchering scams, reference one or more of the same unique identifiers connected to RB's scam:

- a. WS, a resident of Lillington, North Carolina, reported losing \$23,468 worth of cryptocurrency in July and August, 2024 after sending Bitcoin to the address 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV used by a platform identifying itself as BIT and using the URL <https://cdsslt.com>. The description of the scam was consistent with pig butchering.
- b. PT, a resident of Forsyth, Georgia, reported losing \$85,200 in May and June of 2024 after sending USDT to 0x211d18f4262383911500e1298e02c4865e91abe2 used by a platform using the web domain Bit-world.cc. The USDT was forwarded from that address to 0xE073907d67A125DB8Fac7ea4719B3AaB94752D03. The description of the scam was consistent with pig butchering.
- c. TM, a resident of Roebuck, South Carolina, reported in July 2024 having lost at least \$2,000 in cryptocurrency using a site identifying itself as BIT and using the web domain OULARR.com. The description of the scam was consistent with pig butchering.
- d. MW, a resident of Concord, North Carolina, reported in September 2024 having lost \$50,000 to a scam identifying itself as BIT after meeting a woman on a motorcycle enthusiast Facebook group in July. The description of the scam was consistent with pig butchering.
- e. RJ, a resident of Bellevue, Pennsylvania, reported having lost \$50,000 worth of cryptocurrency sent to the Ethereum address 0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34 beginning in April of 20024 using a platform identifying itself as BIT and using the domain bwdcoin.cc. The description of the scam was consistent with pig butchering.
- f. MN, a resident of the Czech Republic, reported losing \$45,000 worth of cryptocurrency between April and September, 2024 after sending it to 0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34 using a site utilizing the domain bit-world.cc. The description of the scam was consistent with pig butchering.

50. Strike searched their records for other victims who sent BTC to the BIT-controlled Bitcoin addresses associated with RB's scam, and provided records identifying the following seven suspected victims who sent a total of 19.55870079 BTC (worth approximately \$1,173,647 at the time of the transactions) between June 28 and August 29, 2024, overlapping with the fraud against RB:

- a. Minneola, Florida resident GF sent a total of 2.95221562 BTC (worth approximately \$191,024) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV on June 28 and July 30, 2024. On September 5, GF reported to law enforcement that he was convinced by a person he met online to wire \$741,769 between September 18, 2023 and July 29, 2024 from his Chase Bank and Wells Fargo accounts to Coinbase, but he was now unable to withdraw and it appeared to be a “fake portal.” This description is consistent with a pig butchering scam.
- b. North Logan, Utah resident KD sent a total of 0.82139442 BTC (worth approximately \$48,950) to 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT on August 28 and 29, 2024. KD reported to law enforcement that he had lost at least \$200,000 between credit card transactions, wire transfers, and cryptocurrency transactions to the platform identifying itself as BIT and using the URL olurr.com. This URL is the same one used by RB.
- c. Jacksonville, FL resident AB sent a total of 2.37151095 BTC (worth approximately \$137,574) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV on July 31 and August 7, 2024. On September 12, AB reported to law enforcement that he had invested \$348,000 via Crypto.com in a supposed investment scam opportunity he was introduced to by someone he met in a chat room and corresponded with on WhatsApp. He reported the incident to law enforcement on September 12 after receiving a call from an FBI agent who warned he might be involved in a scam, and after his stockbroker told him they thought he was being scammed. This description is consistent with a pig butchering scam.
- d. U.S. resident RS sent a total of 0.61050823 BTC (worth approximately \$39,493) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV on July 16, 2024.
- e. U.S. resident DS sent a total of 3.28287845 BTC (worth approximately \$199,716) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV on August 9, 2024.
- f. U.S. resident JK sent a total of 0.21805695 BTC (worth approximately \$12,821) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV on August 12, 2024.
- g. U.S. resident JS sent a total of 6.60996847 BTC (worth approximately \$385,073) to 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV and 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT in five transactions between June 18 and August 30, 2024.

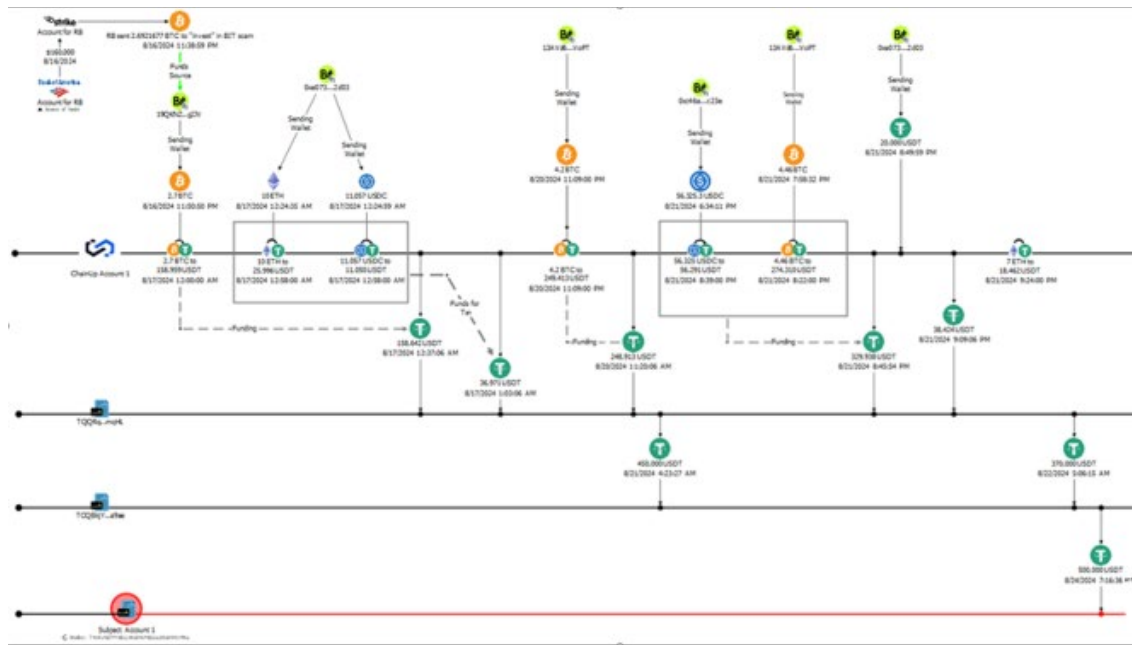
51. In total, the fourteen identified victims reported losses of approximately \$1,798,705.

Affidavit Name	City/State/Country	Loss	Address(es)
RB	Grass Valley, CA	\$167,000	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT 0xE073907d67A125DB8Fac7ea4719B3AaB94752D03 0xC46ABF247b6a0d86FF178561D0893ddD0f00C23e 0xE6626588bAea62C2229783D082d362c9525a1296 TJTWrPyts7ahu22iWupAfeGKDojqy9nLFF
WS	Lillington, NC	\$23,468	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
PT	Forsyth, GA	\$85,200	0x211d18f4262383911500e1298e02c4865e91abe2
TM	Roebuck, SC	\$2,000	Unknown
MW	Concord, SC	\$50,000	Unknown
RJ	Bellevue, PA	\$50,000	0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34
MN	Czech Republic	\$45,000	0xaf25c5a45115F523049F7fc05D4BAD22c60e2F34
GF	Minneola, FL	\$191,024	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
KD	North Logan, UT	\$200,000	13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT
AB	Jacksonville, FL	\$348,000	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
RS	United States	\$39,403	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
DS	United States	\$199,716	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
JK	United States	\$12,821	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV
JS	United States	\$385,073	19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV 13AVd6XBaPxTzDoPRht6VpNw2NT3BWVoPT
Total		\$1,798,705	

C. Facts Leading to the Identification of the Subject Accounts 1 and 2

52. As described below, I used the Blockchain to trace the victim's funds and commingled funds from BIT addresses through a series of transfers between cryptocurrency addresses, known as "hops," to their deposit at Subject Accounts 1 and 2. Once aware of the fraudulent conduct and tracing of victim funds, Tether Ltd., placed a voluntary freeze on the Target Property.

53. The illustration below shows the tracing of funds from RB's bank account to Subject Account 1:



54. The final withdrawal of RB's funds from Strike, sent as an intended investment to the Bitcoin address provided by BIT, occurred on August 16, 2024 in the amount of 2.6921677 BTC (approximately USD value \$158,996.20 at the time of the transaction) and was sent to the Bitcoin address 19QKNZqxJfYwvDu5KnfNXJJGVxBJkogJJV along with a small amount of additional BTC, for a total of 2.7 BTC. Approximately twelve minutes later, it was forwarded from that address to the address 1AD61wBMvt5DRPRV5mG6zAmpT91TGdDrqy in transaction ID 488651a91efb047c752c336834a2706ffc4fa56eb658bdb4e382099a673c7d68.

55. I have reviewed records from ChainUp, a cryptocurrency exchange, showing that this address is a ChainUp customer deposit address identified herein as “ChainUp Account 1.” ChainUp records showed that approximately one minute after the 2.7 BTC was deposited into the account, the user of ChainUp Account 1 attempted to exchange that exact amount of BTC for USDT. The initial exchange was revoked, and a second attempt two minutes later successfully swapped the 2.7 BTC for 158,961.393 USDT. In my training and experience, I know that swaps

of this sort are often conducted with the intention of obfuscating the nature, source, ownership, control, and/or sources of funds.

56. 19 minutes after the swap from BTC to USDT, the account withdrew 158,642.4703 USDT on the Tron network to address TQQRqSbWvoQBDixpZpCUnW8PpZiAbWmqHL in Transaction ID 55fbfb4b296c84677aa125a9c5958598f101696139d71e7d189c98253141463c.

57. There were no other transactions within the account that occurred chronologically between the deposit of the BTC, the exchange for USDT, and the withdrawal of the USDT received from the exchange.

58. Prior to the TQQRqS... address receiving this input, there was only approximately 8,751 USDT in the address. The 158,642.4703 input was combined with two other inputs and three days later, 450,000 USDT (the entire balance except for approximately 3,278 USDT) was withdrawn to the address TCQBkjYHqx6HV2FG2PF2mWor2tULJTae. Before the 450,000 USDT was sent to the TCQBkj address..., that address had a USDT balance of zero. During approximately the following 27 hours, 50,000 USDT was withdrawn to a different address, another 370,000 USDT was received into the address, and then 500,000 USDT was sent to the address TNihvNZfFYdSjLWyEHIPXQ2u28oXHN1PNu, previously identified as Subject Account 1.

Voluntary Freeze of the Target Property by Tether Ltd.

59. Further analysis of the transaction history of the involved cryptocurrency addresses indicated that Subject Account 1 and another Tether address on the Tron network, TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF (previously identified as Subject Account 2), had a history of receiving inputs from addresses attributed to the BIT investment scam, after the

cryptocurrency had been moved in patterns consistent with the manner in which RB's funds were moved.

60. On September 4 and September 5, respectively, Tether placed a voluntary freeze on the USDT in Subject Accounts 1 and 2. At the time the accounts were frozen, the USDT balances in those accounts were 500,000 USDT and 900,000.145687 USDT, respectively.

Responses to the Freeze of the Target Property

61. Additional transaction activity occurred within Subject Accounts 1 and 2 after the addresses were "blocklisted" (frozen) by Tether Ltd.

62. In Subject Account 1, no other transaction activity had previously occurred other than the 500,000 USDT input. No TRX had ever been deposited into the account. TRX is the native currency of the Tron network and is necessary to pay the transaction fee for any withdrawal of USDT. On September 10, 2024 at 14:51:03 UTC, 70 TRX was deposited into the account. On that day at 14:51:45, a USDT transaction was attempted but failed, and a series of additional USDT transaction attempts followed. This behavior is consistent with the owner of the account attempting to withdraw USDT from the account and learning that withdrawals were being prevented.

63. Subject Account 2 had a more extensive transaction history with prior TRX inputs in the account. On September 10, 2024 at approximately 13:21:03 UTC (approximately 1.5 hours before the failed USDT transactions in Subject Account 1), a series of failed USDT transactions occurred in Subject Account 2. This behavior is consistent with the owner of the account attempting to withdraw USDT from the account and becoming aware that withdrawals were being blocked.

64. Tether Ltd. informed me that on September 11, 2024 an individual using the name “linda” contacted Tether from the email address linda11661166[.]gmail.com claiming ownership of both addresses in the Target Property.

65. I recognized the name “Linda” as the name used by the person who led RB to invest on the BIT platform.

66. On September 17, 2024 at 3:31 PM I received an email from linda11661166[.]gmail.com stating, “TNihvNZfFYdSjLWyEHIPXQ2u28oXHN1PNu This is my address and I would like to know how I can get my funds unfrozen and be able to transfer my assets normally, thank you.” The TNihvNZ... address is Subject Account 1.

67. Three minutes later I received an email from zjing6950[.]gmail.com stating, “TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF This is my address and I would like to know how I can get my funds unfrozen and be able to transfer my assets normally, thank you.” The TTscFq... address is Subject Account 2.

68. I noted that the language used in the two emails was identical, and the first email was sent from the email address that had initially claimed ownership of both addresses. Since then, I have received several emails from other email addresses claiming ownership of one or both of the Subject Accounts. I asked each requesting party to screen shot or take a video of them operating the wallet, to verify their ownership claim. One individual, using an email address different than those identified above, responded with a video that appeared to show a recording of a mobile phone with a Chinese language interface being used to access a wallet controlling Subject Account 2. On November 4, 2024, I replied to that user inquiring about their location to facilitate an in-person meeting. There was silence and no reply until December 24, when the user responded, claiming to be “from China and currently in Hong Kong” and asking to

remove the restrictions on the address. On December 31, I replied to that email and inquired about finding a mutually agreeable location to meet and discuss the origin of the funds. As of today's date, the user has not replied.

Post-Freeze Changes to the USDT Balances in Subject Accounts 1 and 2

69. Subject Account 1 received another deposit of 1.2 USDT on September 30, 2024.

70. Subject Account 2 received additional inputs of USDT on September 3 (254,015 USDT), September 8 (100,000 USDT), and September 10 at 19:39:42 UTC (100 USDT).

71. As of the writing of this affidavit, the USDT balances in these accounts are as follows:

- a. 500,001.2 USDT in Subject Account 1
- b. 1,000,100.145687 USDT in Subject Account 2

B. Laundering Fraud Proceeds Collectively to Subject Accounts 1 and 2

72. Using public blockchains and records obtained from cryptocurrency exchanges I used a "last in, first out" (or "LIFO") tracing methodology, in which the cryptocurrencies from immediately preceding transfers are the first withdrawn in subsequent transfers before any other funds, to examine the source of the USDT received by Subject Accounts 1 and 2.

73. The analysis focused on identifying the source all significant USDT deposits into the accounts (excluding *de minimis* amounts, specifically one deposit each of 1.20 USDT, 1.00001 USDT, and 100 USDT), including those USDT assets that remain frozen after other assets were withdrawn.

74. The analysis showed that various amounts of Bitcoin, Ether, USDT, and USDC cryptocurrency moved from the addresses attributed to BIT using some combination of multiple hops and decentralized swaps on the blockchain, rapid "pass-through" movement through

exchange accounts without converting to a different cryptocurrency or network, rapid “pass-through” movement through exchange accounts with conversion to a different cryptocurrency or network, the use of more than one exchange in sequence, re-aggregation after the movement through exchange accounts, and culminating in transfer to Subject Accounts 1 and 2.

75. During the course of the investigation I received records from the cryptocurrency exchanges ChainUp and 100ex pertaining to two involved ChainUp accounts and four involved 100ex accounts. Analysis of the account records indicated that the vast majority of funds received into at least five of these accounts were attributable to addresses attributed to the BIT scam. The customer due diligence records indicated that all of the account holders were from the People’s Republic of China, and the background of those photographs in which account holders were holding up their identification cards showed the photos were taken in what appeared to be the same corner of the same room, based on the shadowing and the coloration of the walls (see below). In two of the photos, what appears to be the same mark on the wall can be seen. The transaction patterns within the accounts were similar (deposits of BTC, ETH, USDC and USDT with most of the assets swapped to USDT on the Tron network). Withdrawals from both ChainUp accounts were nearly all to the same withdrawal addresses. Based on these facts, I believe at least three of the intermediary ChainUp and 100ex accounts were operated by the same organization and were used primarily for the laundering of the proceeds of cryptocurrency fraud.



ChainUp 1



ChainUp 2



100ex 3

76. Based on my training and experience, I know that criminals will often conduct an otherwise unnecessary number of transactions in the transfer of funds in an effort to layer ill-gotten funds to ultimately conceal or disguise the nature, location, source, ownership, or control of those proceeds when they are ultimately transferred into a cryptocurrency exchange. The number of hops and swaps involved is a strong indication that the movement of funds was performed in a manner meant to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity, to wit, wire fraud.

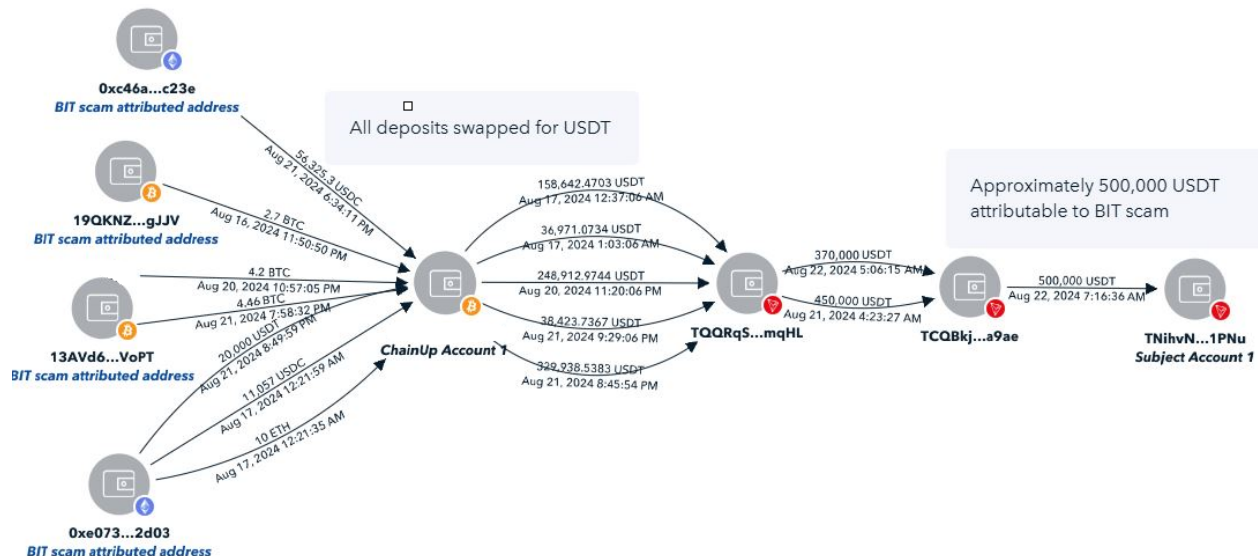
77. Based on the aforementioned LIFO principle, the undersigned calculated that in aggregate, approximately 100% of the total historical USDT inputs into Subject Account 1 (500,000 out of 500,001.2 USDT) and approximately 70% of the total historical USDT inputs into Subject Account 2 (approximately 1,788,453 out of 2,554,119 USDT) could be traced back to addresses attributed to the BIT scam and similar pig butchering scams.

78. Furthermore, also based on the aforementioned LIFO principle, the undersigned calculated that in aggregate, approximately 100% of the current, frozen balance of Subject Account 1 (500,000 out of 500,001.2 USDT) and conservatively no less than 26% of the current, frozen balance of Subject Account 2 (255,970 out of approximately 1,000,100 USDT),

representing in aggregate approximately 50% of the current balance of the two accounts, could be traced back to addresses attributed to the BIT scam and similar pig butchering scams based on the information currently available. The trackways of each significant input into Subject Accounts 1 and 2 are briefly summarized below.

Subject Account 1, Deposit Occurred 8/22/2024

79. A 500,000 USDT deposit into Subject Account 1 occurred on August 22, 2024 that originated in its entirety from addresses attributed to the BIT scam. The source of those assets is illustrated below. In summary, cryptocurrency assets in the form of USDT, USDC, ETH, and BTC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1, where they either passed through as USDT or were swapped for USDT. They were then withdrawn to TQQRqS..., where they were aggregated and forwarded to TCQBkj..., where they were further aggregated and then sent in a single deposit to Subject Account 1 after some of the funds in TCQBjk... were sent elsewhere.

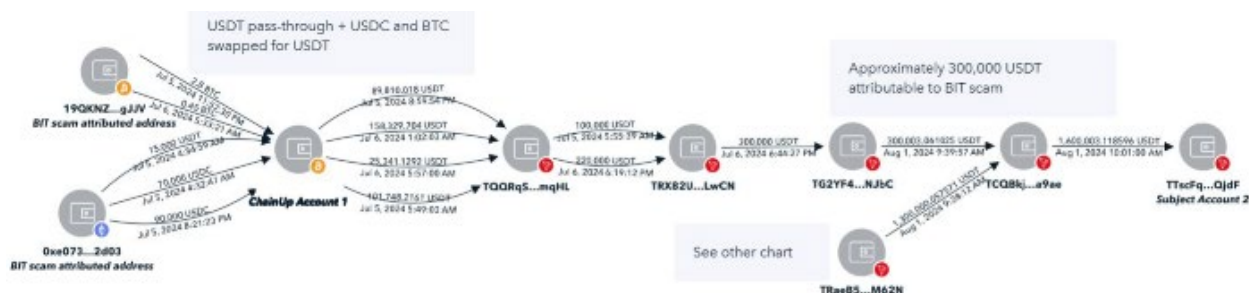


Subject Account 2, Deposit Occurred 8/1/24 (Segment 1 of 2)

80. A 1,600,003 USDT deposit into Subject Account 2 occurred on August 1, 2024 that predominantly originated from addresses attributed to the BIT scam. There were two component inputs included in this deposit: one input of 300,003 USDT (segment 1 of 2), and another of 1,300,000 USDT (segment 2 of 2).

81. Segment 's sources are illustrated below. In summary, cryptocurrency (USDC, USDT, and BTC) was sent from BIT scammed addresses directly to ChainUp Account 1, where they were swapped for USDT. They were then withdrawn to TQQRqS..., where they were aggregated and forwarded to TRX82U..., where they were aggregated and forwarded to TG2YF4... after some assets were sent elsewhere, and then combined with segment 2 and forwarded to Subject Account 2.

82. The illustration below demonstrates the movement of these funds (segment 1 of 2) from attributed BIT scam addresses to Subject Account 2, of which approximately 300,000 USDT deposit is attributable to the BIT scam:



Subject Account 2, Deposit Occurred 8/1/24 (Segment 2 of 2)

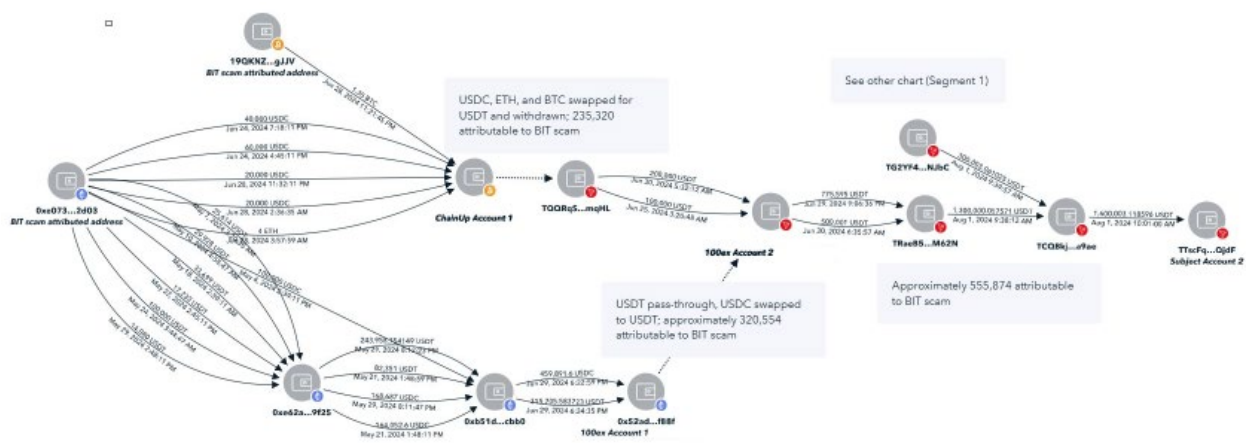
83. The 1,300,000 USDT segment of the 1,600,003 USDT deposit into Subject Account 2 that occurred on August 1, 2024 also originated in large part from addresses attributed to the BIT scam. The movement of funds occurred as follows, in summary:

- a. In one path, 100ex Account 1 received deposits of USDC and USDT indirectly (through either one or two hops) from an address attributed to the

BIT scam. 100ex Account 1 swapped the USDC for USDT, combined these deposits with other deposits, and transferred the USDT to 100ex Account 2, where approximately 320,554 USDT of the transferred assets were traceable to addresses attributed to the BIT scam. (See below for a description of the continued path from 100ex Account 2.)

- b. In a second path, cryptocurrency assets in the form of USDC, ETH, and BTC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1. There they were swapped for USDT and withdrawn to TQQRqS..., where they were aggregated and forwarded to 100ex Account 2, where approximately 235,320 USDT of the transferred assets were traceable to addresses attributed to the BIT scam. (See below for a description of the continued path from 100ex Account 2.)
- c. In two transactions on June 30, 2024, withdrawals 500,001 USDT and 775,595 USDT were made from 100ex Account 2 to TRaeB5..., of which approximately 555,874 USDT originated from addresses attributed to the BIT scam. These assets were forwarded from TRaeB5... where they were combined with other assets and forwarded to TCQBkj..., where they were aggregated with segment 1 and sent to Subject Account 2.

84. The illustrations below demonstrate the movement of these funds from attributed BIT scam addresses to Subject Account 2:

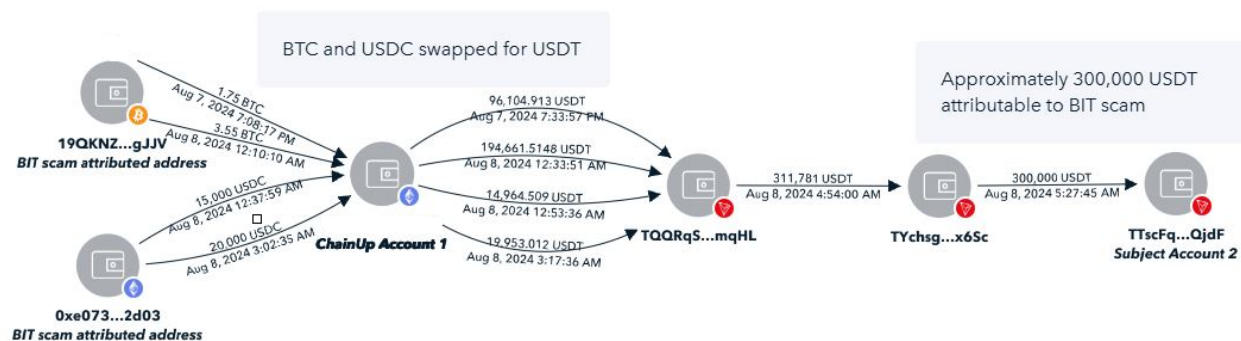


Subject Account 2, Deposit Occurred 8/8/24

85. A 300,000 USDT deposit into Subject Account 2 occurred on August 8, 2024 that originated in large part from addresses attributed to the BIT scam. In summary, cryptocurrency

assets in the form of BTC and USDC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1, where they were swapped for USDT. They were then withdrawn to TQQRqS..., where they were aggregated and forwarded in a single transaction to TYchsg..., from which some was sent to another destination and the remainder was forwarded to Subject Account 2. Approximately 300,000 USDT of that deposit was traceable to addresses attributed to the BIT scam.

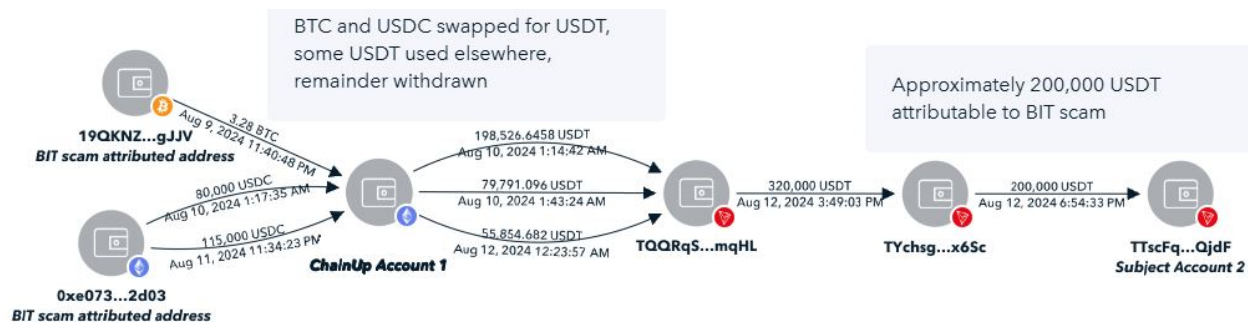
86. The illustration below demonstrates the movement of these funds from attributed BIT scam addresses to Subject Account 2:



Subject Account 2, Deposit Occurred 8/12/24

87. A 200,000 USDT deposit into Subject Account 2 occurred on August 12, 2024 that originated in large part from addresses attributed to the BIT scam. In summary, cryptocurrency assets in the form of BTC and USDC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1, where they were swapped for USDT. Some of the USDT was sent elsewhere and the balance was withdrawn to TQQRqS..., where they were aggregated and forwarded to TYchsg..., from which some was sent to another destination and the remainder was forwarded to Subject Account 2. Approximately 200,000 USDT of that deposit was traceable to addresses attributed to the BIT scam.

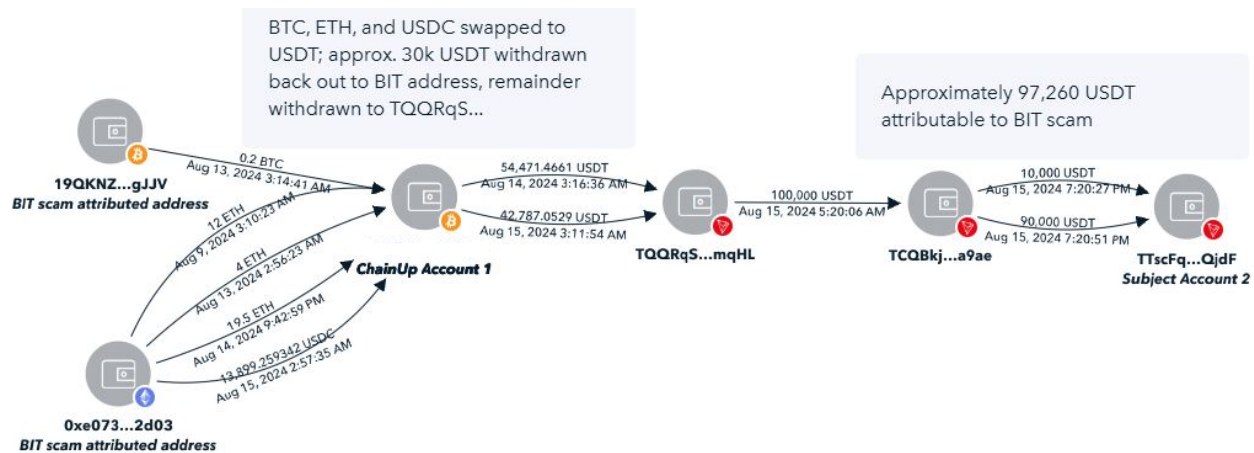
88. The illustration below demonstrates the movement of these funds from attributed BIT scam addresses to Subject Account 2:



Subject Account 2, Deposits Occurred 8/15/24

89. Two deposits of 10,000 and 90,000 USDT into Subject Account 2 occurred on August 15, 2024 that originated in large part from addresses attributed to the BIT scam. In summary, cryptocurrency assets in the form of ETH, BTC, and USDC were sent from addresses attributed to the BIT scam directly to ChainUp Account 1, where they were swapped for USDT. They were then withdrawn to TQQRqS..., where they were aggregated and forwarded in a single transaction to TCQBkj..., from where they were sent in two deposits to Subject Account 2. Approximately 97,260 USDT of that deposit was traceable to addresses attributed to the BIT scam.

90. The illustration below demonstrates the movement of these funds from attributed BIT scam addresses to Subject Account 2:



Subject Account 2, Deposit Occurred 9/3/24

91. A deposit in the amount of 254,015 USDT occurred on 9/3/24 that originated in large part from addresses attributed to the BIT scam. In summary, cryptocurrency assets in the form of USDC and BTC were sent directly from addresses attributed to the BIT scam to 100ex Account 3, where they were swapped for USDT and then withdrawn to the TKdchh.... There they were combined and forwarded (along with additional USDT) to TCQBkj..., where they were combined with additional USDT and forwarded to Subject Account 2. Approximately 235,542 USDT of that deposit was traceable to addresses attributed to the BIT scam.

92. The illustration below demonstrates the movement of these funds from attributed BIT scam addresses to Subject Account 2:



Subject Account 2, Deposits Occurred 9/8/24

93. A deposit in the amount of 100,000 USDT occurred on 9/8/24 that originated in large part from addresses attributed to the BIT scam. In summary, cryptocurrency assets in the form of USDC were sent directly from an address attributed to the BIT scam to 100ex Account 3, where they were swapped for USDT and then withdrawn to the TKdchh... address. There they were combined and forwarded (along with additional USDT) to TTQ15w..., where some of the assets were combined with additional USDT and the balance was sent to Subject Account 2. Approximately 99,778 USDT of that deposit was traceable to addresses attributed to the BIT scam.

94. The illustration below demonstrates the movement of these funds from attributed BIT scam addresses to Subject Account 2:



C. GLEHFX.com Wire Fraud Scheme

95. During the course of this investigation another victim, a 38-year-old resident of San Jose referred to herein by his initials as “RM,” reported falling victim to a scheme with the following similarities to the BIT scheme targeting RB:

- a. RM was involved in the scam during the same period of time as RB;
- b. RM met an Asian woman online who claimed to be from another city on West Coast;
- c. The suspect corresponded with RM using some of the same communication applications used to communicate with RB;
- d. The suspect used the pretext of their relationship to introduce him to a speculative short-term trading opportunity utilizing cryptocurrency in which he interacted with a web site and a decentralized wallet application;

- e. The suspect claimed to be advised by an uncle who was a successful trader and led RM to believe that she had added funds to his account;
- f. RM funded the purported investments using cryptocurrency purchased on an exchange after being coached through the process of creating the exchange account and wiring funds from his bank accounts;
- g. RM was led to believe, through interaction with the app, that his investments had grown substantially in value; and,
- h. RM was led to believe that his account had been frozen and he had to pay an additional substantial fee to access his funds before he realized he was being defrauded.

96. RM's attempted investment in the GLEHFX platform is based on RM's statements and information viewable on public blockchains.

97. In or about June of 2024, RM connected with an individual named Chen YUE on Tinder. They began an online relationship and generally communicated on WhatsApp and Line. RM described YUE as an attractive Chinese female that spoke fair English but was not a native speaker. She appeared to be in an apartment and claimed that she was living in the hills of Los Angeles. RM was not provided any proof that she was actually in Los Angeles. RM said that sometimes their conversations had to end because what appeared to be a servant entered the room where she was video chatting.

98. In July of 2024, YUE encouraged RM to begin investing in an online App called Evjorerjrb, an Android-based app also associated with a web site GLEHFX.com. The application and webpage purport to make their users money through short-term leveraged short-selling gold contracts.

99. RM funded the gold trading account with payments of ETH. YUE guided him through the process of opening a Kraken account. RM funded his Kraken account with transfers from both his Bank of America account and his Wells Fargo account.

100. Prior to interacting with this website, RM had little knowledge and no experience in trading cryptocurrency. YUE said that she was being advised by a rich uncle who was successful in gold trading. RM was led to believe that YUE had also added \$85,000 into the account.

101. Between August 9 and 17, 2024, RM made four deposits from his Kraken account to the Evjorerjb/GLEHFX.com application totaling approximately 42.143 ETH, which at the time of the transactions had an approximate USD value of \$109,556. RM identified the transactions which investigators located on the Ethereum blockchain.

102. The online account made it appear as if their investment had made a \$480,000 profit in a matter of a few weeks.

103. After RM told YUE that he had no additional money to invest and that he wanted to withdraw funds, the website's account administrator informed RM on or about August 23, 2024 via an online message that he was being suspected of money laundering. He was requested to deposit an additional \$85,000 "to lift the account", and then the deposit would be returned to him.

104. RM became suspicious and began questioning YUE. He went to a residential address in San Jose that YUE had told RM that she owned as an investment, but the residents at that address had never heard of YUE. At that point RM realized he had been defrauded and reported the suspected crime to law enforcement.

Facts Leading to the Identification of Subject Account 3

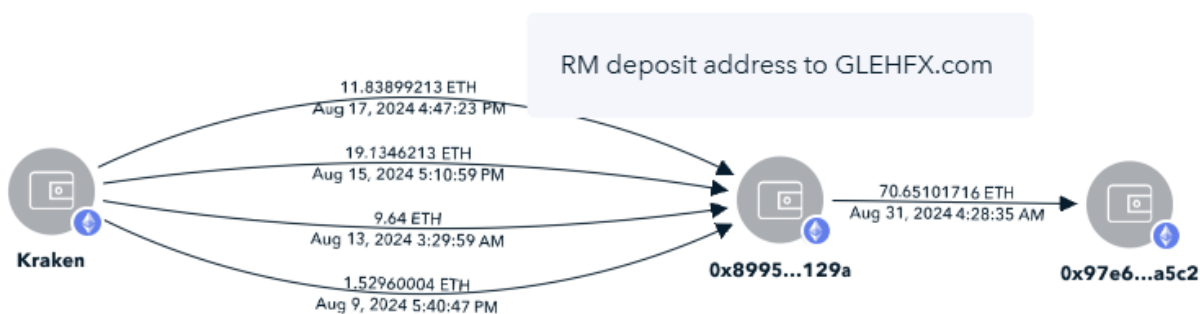
105. As described below, investigators traced the victim's funds and other funds from the addresses attributable to GLEHFX.com on the publicly available blockchain through a series

of transfers between cryptocurrency addresses, known as “hops,” to their arrival at Subject Account 3.

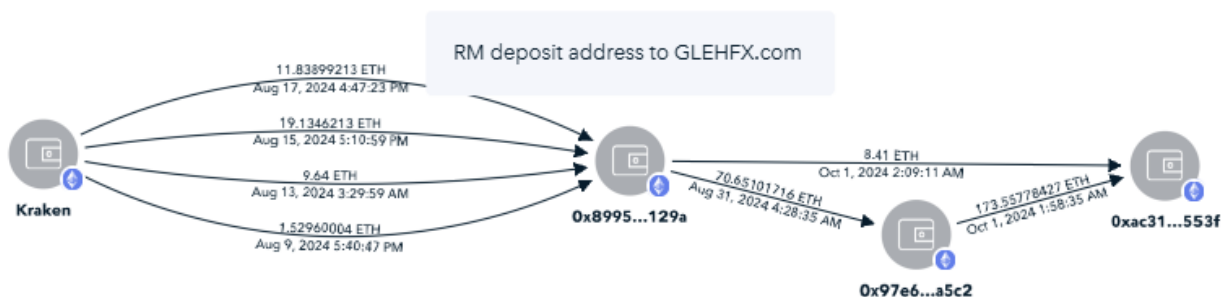
106. Investigators brought the account to the attention of Tether Ltd., which placed a voluntary freeze on Subject Account 3.

Laundering of the Proceeds of the Theft from RM and Discovery of Additional Victims

107. RM “invested” in the GLEHFX.com application by sending ETH from his Kraken account to the Ethereum address 0x899542876793412ba19D0b3265D01cea8F9E129a (which was provided to him by the scammers) in the transactions illustrated below, after which it was comingled with other funds and forwarded to the 0x97e6... address as illustrated below:



108. After the victim funds were sent to 0x97e6..., they were consolidated with other funds and sent to 0xaC319FBA26610b7685Cb2563D00Ef99f51A7553f. This address also had direct deposits from the address to which RM had sent his funds on October 1, 2024, as illustrated below:



109. Investigators located four additional reports made to iC3 establishing that the 0x97e6... address had received funds directly from victims involved in several similar Pig Butchering scams:

- a. A resident of Clearwater, Florida reported a loss of \$30,000 worth of cryptocurrency that occurred on or about May 13, 2024. The victim reported a woman he met online directed him in opening an account with a site called “Golden Elephant” to which he had sent approximately \$30,000 worth of cryptocurrency to the address 0x6ADb699b26e77F470a8F2bE0298957C4f2290A35. He was later unable to withdraw his funds and realized it was a scam.
- b. A resident of San Francisco, California reported a loss of \$25,000 worth of cryptocurrency that occurred on or about October 11 through 18, 2024. The victim reported that a woman he met through a wrong number call convinced him to invest cryptocurrency in a site accessed through an iPhone application called “sdcfskdvt.” At the suspect’s direction, he sent cryptocurrency to the address 0xc296E0E97b4E17d213df2BC044BE356C0499a332. He later realized it was a scam when he could not withdraw any funds and deposits that were purportedly made by the suspect to the victim’s account for his benefit did not appear on the blockchain.
- c. A resident of Reno, Nevada reported a loss of \$118,400 worth of cryptocurrency that occurred on or about March 19 and 20, 2024. The victim reported that he was befriended by a female met through a wrong number text message. She convinced him to take out a loan and invest through a web site using the URL DMMtopbitus.com. The victim sent the funds to the Ethereum address 0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86 at the direction of the suspect and learned it was a scam after he could not withdraw his funds and was asked to prepay “taxes.”
- d. A resident of Leander, Texas reported a loss of \$46,000 that occurred between approximately January 23 and February 7, 2024. The victim reported being befriended by a female met through a wrong number text message. She convinced the victim to invest in a website at the address DMMtopbitus.com, and he did so by depositing ETH to the address 0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86 and realized it was a scam after being asked to prepay his taxes.
- e. A resident of McDonough, Georgia reported a loss of \$133,580 that occurred on or about June 21, 2024. The victim reported having sent cryptocurrency to a fraudulent platform named DMM Bitcoin, at the direction of a friend he met through a messaging app. The victim was directed to send ETH to the address

0x1D95B2286cC4E8046bb868A1F20b2EC7CcafaB9F. The victim later realized this was a scam.

110. In total, these six identified victims reported losses of approximately \$462,536.

Affidavit Name	City/State/Country	Loss	Address(es)
RM	San Jose, CA	\$109,556	0x899542876793412ba19D0b3265D01cea8F9E129a
O-1	Clearwater, FL	\$30,000	0x6ADb699b26e77F470a8F2bE0298957C4f2290A35
O-2	San Francisco, CA	\$25,000	0xc296E0E97b4E17d213df2BC044BE356C0499a332
O-3	Reno, NV	\$118,400	0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86
O-4	Leander, TX	\$46,000	0x7255E1fba48783d1AD5f8b7af1ceB0621d67AD86
O-5	McDonough, GA	\$133,580	0x1D95B2286cC4E8046bb868A1F20b2EC7CcafaB9F
Total		\$462,536	

111. The proceeds of all these scams were forwarded to the 0xaC319FB address that had received RM's funds. That address had also received fund directly from the San Francisco victim described above. The paths of funds from the victims' exchange accounts to the 0xaC319FB... address are illustrated below.



112. On October 13, 2024, this consolidation address sent two deposits totaling approximately 292.8355 ETH to the address 0x366e2BEef3635b644D4698E33Ef557449ABeC8E7 ("Subject Account 3"). This address had

been funded solely by these two transactions. On November 18, 2024, approximately 92 ETH was sent in two transactions to a decentralized finance application and converted within the same address to approximately 285,157.35 USDT.

113. On November 18, 2024, investigators brought the suspected illicit activity to the attention of Tether Ltd. At that time the USDT balance in Subject Account 3 was approximately 281,158 USDT.

Voluntary Freeze of Subject Account 3 by Tether Ltd., and Subsequent Account Activity

114. On November 20, 2024, Tether placed a voluntary freeze on the USDT in Subject Account 3.

115. By the time the account was “blocklisted” (frozen), two withdrawals of USDT had been conducted, leaving a USDT balance of only 0.547356 USDT.

116. As noted, the Ethereum address containing that remaining USDT had been used to swap ETH for USDT using decentralized finance applications. That address still contained a substantial amount of ETH attributable to the identified scam deposit addresses. As a result, the account remained voluntarily blocklisted by Tether. This blocklisting allowed new deposits of USDT, but not withdrawals, to occur.

117. On December 1, 2024, Subject Account 3 sent 348.8 ETH to a decentralized finance application and received 1,285,539.809879 USDT in exchange. The freeze placed by Tether Ltd. remains in place.

118. On December 26, 2024, Tether Ltd. informed investigators that they had been contacted by someone claiming ownership of Subject Account 3 who provided only the name “rui” and the email address from the domain 163.com. Tether provided them with contact information for a REACT investigator but no contact has been received from that individual.

119. As of the writing of this affidavit, the USDT balances in Subject Account 3 is 1,285,540.357235.

B. Laundering Fraud Proceeds Collectively to the Target Property

120. Using public blockchains and records obtained from cryptocurrency exchanges I used the aforementioned LIFO tracing methodology to examine the source of the USDT received by Subject Account 3.

121. All of the USDT ever received by Subject Account 3 was derived from ETH deposits into the account, whereby the ETH deposited into the account was swapped within the account for USDT using a decentralized finance application.

122. There were three deposits of ETH into the account:

- a. A deposit of 0.1 ETH on October 13, 2024
- b. A deposit of 292.735563 ETH on October 13, 2024
- c. A deposit of 147.588713 ETH on November 28, 2024.

123. The analysis focused on identifying the source these ETH deposits.

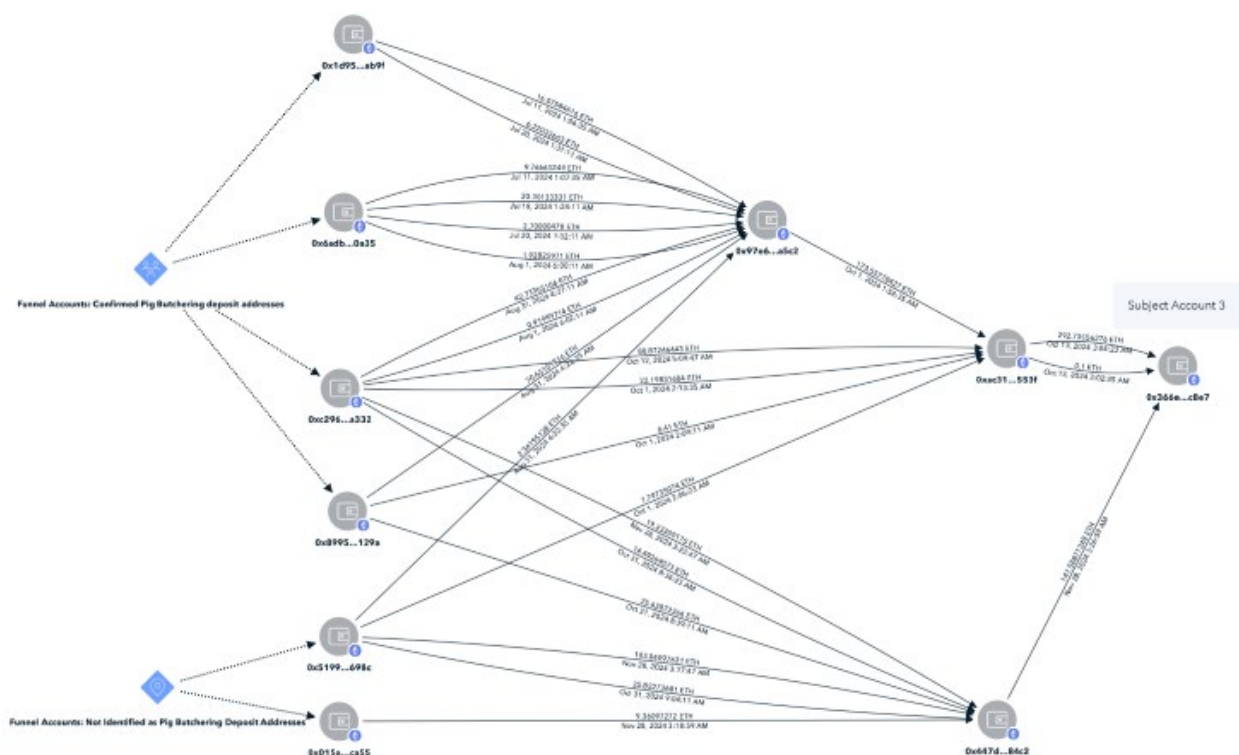
124. All of the ETH inputs received by Subject Account 3 arrived via six “funnel accounts,” which collected ETH from a variety of sources and forwarded it via either one or two “hops” to Subject Account 3.

125. Based on the information currently available, four of those six “funnel accounts” have been identified by victim reporting as scam deposit addresses, as described above.

126. Based on my training and experience, I know that criminals will often conduct an otherwise unnecessary number of transactions in the transfer of funds in an effort to layer ill-gotten funds to ultimately conceal or disguise the nature, location, source, ownership, or control of those proceeds when they are ultimately transferred into a cryptocurrency exchange. The

aggregation of illicit funds in “funnel accounts” and the forwarding of the funds through one or more hops to an aggregation address where the funds are swapped for another type of cryptocurrency is an indication that the movement of funds was performed in a manner meant to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity, to wit, wire fraud.

127. The paths of the inputs into Subject Account 3 from the “funnel accounts” are illustrated below:



128. Based on the aforementioned LIFO principle, the undersigned calculated that in aggregate, at least approximately 72% of the total historical ETH inputs into Subject Account 3 (317.9645 of the total 440.3243 ETH received), and therefore 72% of the total historical USDT inputs into the account, could be traced back to addresses attributed to Pig Butchering scams.

129. Furthermore, also based on the aforementioned LIFO principle, the undersigned calculated that in aggregate, conservatively no less than approximately 51% of the current,

frozen balance of Subject Account 3 (approximately 659,710 out of 1,285,540 USDT) could be traced back to addresses attributed to Pig Butchering scams based on the information currently available.

SEIZURE PROCEDURE FOR THE TARGET PROPERTY

130. There is probable cause to believe the funds held in the Target Property are subject to civil and criminal forfeiture, as proceeds of wire fraud and involved in illegal money laundering.

131. Law enforcement intends to work with Tether to seize the funds associated with the Target Property. In sum, the accompanying warrants would be transmitted to Tether, and Tether will “burn” (*i.e.*, destroy) the addresses at issue (and by extension the USDT tokens associated with them). Tether would then reissue the equivalent amount of USDT tokens associated with the Target Property and transfer that equivalent amount of USDT to a government-controlled wallet. The seized currency will remain in the custody of the U.S. government during the entire pendency of the forfeiture proceedings, to ensure that access to, or manipulation of, the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

CONCLUSION

132. Based on information derived from the foregoing investigation, there is probable cause to conclude that the Target Property contains the proceeds of a wire fraud scheme performed in violation of Title 18, United States Code, Section 1343. Those proceeds, which include 1,415,680 USDT from the Target Property, are subject to seizure and forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section

2461(c). Moreover, there is probable cause to believe that the proceeds of other schemes, Pig Butchering or otherwise, are also present in the Target Property. Finally, there is further probable cause to believe that a greater amount of funds constitute property involved in money laundering transactions, to wit: the entire USDT balance of the Target Property. These funds are accordingly subject to forfeiture and seizure pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and 982(a)(1). Accordingly, I respectfully request that warrants be issued authorizing the seizure of the Target Property with the goal of returning these funds to the victims impacted by the various scams implicated in this investigation.

133. I submit that a protective or restraining order issued pursuant to 21 U.S.C. § 853(e) would be insufficient to ensure the availability of the funds in the Target Property for forfeiture. Cryptocurrency can be transferred faster than traditional bank funds, and once transferred, generally cannot be recalled to an original wallet. Moreover, there is a risk that the funds may be moved to a location where no forfeiture or seizure would be possible, at which point the funds could be further laundered into a “privacy” (i.e. untraceable) cryptocurrency. Thus, I submit that seizure warrants are the only means to reasonably assure the availability of the funds in the Target Property for forfeiture.

134. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Respectfully submitted,


/s/

DAVID BERRY
Criminal Investigator, Santa Clara County
Office of the District Attorney
Special Deputy U.S. Marshal,
U.S. Secret Service Cyber Fraud Task Force

Reviewed and approved as to form

/s/ Kevin C. Khasigian
Kevin C. Khasigian
Assistant U.S. Attorney

Sworn before me and signed telephonically
on this 13 day of January 2025.



Hon. Carolyn K. Delaney
United States Magistrate Judge

ATTACHMENT A: PROPERTY TO BE SEIZED

Pursuant to this warrant, Tether shall provide the law enforcement officer/agency serving this document with the equivalent amount of USDT tokens that are currently associated with the virtual currency addresses referenced below (*i.e.*, 2,785,641.702922 USDT). Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency addresses referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency wallet. Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

- 500,001.2 USDT held in the Tron account
TNihvNZfFYdSjLWyEHIPXQ2u28oXHN1PNu
- 1,000,100.145687 USDT held in the Tron account
TTscFqjCSFTpKufe8jjH653JmgYCHvQjdF
- 1,285,540.357235 USDT held in the Ethereum account
0x366e2beef3635b644d4698e33ef557449abec8e7

United States District Court

EASTERN District of CALIFORNIA

In the Matter of the Seizure of
(Briefly describe the property to be seized)

1,285,540.357235 USDT held in the Ethereum account
0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7.

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

CASE NUMBER: 2:25-sw-0032 CKD

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the BRITISH VIRGIN ISLANDS be seized as being subject to forfeiture to the United States of America. The property is described as follows:

**1,285,540.357235 USDT held in the Ethereum account
0x366e2BEeF3635b644D4698E33Ef557449ABeC8E7.**

The property is subject to seizure pursuant to 18 U.S.C. §§ 981(b) and 982(b), and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), and 982(a)(1), and 28 U.S.C. § 2461(c).

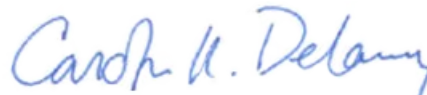
I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property within 14 days in the daytime 6:00 a.m. to 10:00 p.m. You must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to CAROLYN K. DELANEY or Any U.S. Magistrate Judge in the Eastern District of California.

January 13, 2025 at 5:52 pm
Date and Time Issued

Sacramento, California
City and State


Judge's signature

Carolyn K. Delaney, U.S. Magistrate Judge
Printed name and title

AO 109 (Rev. 11/13) Warrant to Seize Property Subject to Forfeiture (Page 2)

RETURN

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken:

CERTIFICATION

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

Subscribed, sworn to telephonically, and returned before me this date.

U.S. Judge or Magistrate_____
Date